

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-305855

(43)Date of publication of application : 02.11.2000

(51)Int.Cl.

G06F 12/14

G11B 20/10

(21)Application number : 2000-039261

(71)Applicant : SONY CORP

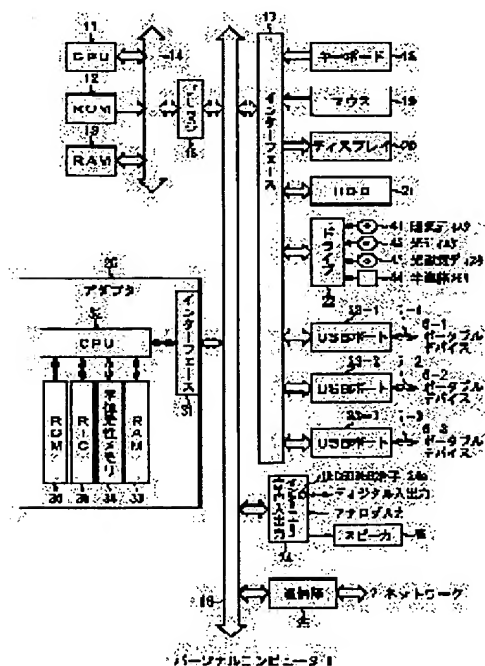
(22)Date of filing : 17.02.2000

(72)Inventor : KAWAKAMI TATSU
ISHIGURO RYUJI
TANABE MITSURU
EOMO YUICHI

(30)Priority

Priority number : 11039223 Priority date : 17.02.1999 Priority country : JP

(54) INFORMATION PROCESSOR, ITS METHOD AND PROGRAM STORING MEDIUM



(57)Abstract:

PROBLEM TO BE SOLVED: To surely prevent data from being illegally copied.

SOLUTION: In the case of transferring music data recorded in an HDD 21 to a flash memory in a portable device 6 and storing the data in the memory, a CPU 11 judges whether the device 6 has a function for protecting various conditions such as a reproducing condition, a reproduction charging condition and a copying condition or not, and only when the device 6 has the function, transfers and stores the music data in the flash memory.

CLAIMS

[Claim(s)]

[Claim 1] When transferring said data stored in an are recording means to store data, a maintenance means to hold the conditions of the utilization time of said data stored in said are recording means, and said are recording means to other equipments, said -- others -- equipment whether the conditions of the utilization time of said data can be satisfied with a judgment means to judge The information processor characterized by including a transfer means to transfer said data stored in said are recording means to equipment besides the above with the conditions of the utilization time of said data currently held at said maintenance means, based on the judgment result of said judgment means.

[Claim 2] The conditions of the utilization time of said data are a playback restriction and an information processor according to claim 1 characterized by including accounting conditions or a copy restriction at the time of playback.

[Claim 3] When transferring said data stored by processing of the are recording step which stores data, the maintenance step holding the conditions of the utilization time of said data stored by processing of said are recording step, and said are recording step to other equipments, said -- others -- equipment whether the conditions of the utilization time of said data can be satisfied with the judgment step to judge The information processing approach characterized by including the transfer step which transfers said data stored by processing of said are recording step to equipment besides the above with the conditions of the utilization time of said data held by processing of said maintenance step based on the judgment result in said judgment step.

[Claim 4] When transferring said data stored by processing of the are recording step which stores data, the maintenance step holding the conditions of the utilization time of said data stored by processing of said are recording step, and said are recording step to other equipments, said -- others -- equipment whether the conditions of the utilization time of said data can be satisfied with the judgment step to judge Based on the judgment result in said judgment step, said data stored by processing of said are recording step with the conditions of the utilization time of said data held by processing of said maintenance step The program storing medium by which the program which the computer characterized by including the transfer step transferred to equipment besides the above can read is stored.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention certainly relates to a program storing medium at the information processor and approach of having enabled it to prevent the unjust duplicate, and a list, also when transferring the data stored in the information processor and the approach, and the

list about the program storing medium.

[0002]

[Description of the Prior Art] Recently, it follows on the spread of digital technique, and various kinds of data, such as music data and image data, have come to be recorded or reproduced by the record medium in digital one. Consequently, even if it carries out a multiple-times copy, it has become possible to obtain the data with which image quality or tone quality does not deteriorate.

[0003]

[Problem(s) to be Solved by the Invention] However, if digital technique progresses in this way, the following problems will occur.

[0004] (1) for example, the case where digital music data are copied to the hard disk of a personal computer from a compact disk (CD) -- the music data from CD -- as it is -- or since compression coding is carried out and it is recorded on a hard disk, a duplicate will be able to be illegally distributed in large quantities through networks, such as the Internet, for example.

[0005] (2) Since there is no limit in the count of the copy when copying digital music data to the hard disk of a personal computer from CD, a duplicate will be distributed in large quantities.

[0006] (3) Since the original digital music data remain in a hard disk even after moving when moving the digital music data in the hard disk of a personal computer to the device of the exteriors, such as a portable device, there is a possibility that a duplicate can distribute in large quantities.

[0007] (4) In order to prevent the above-mentioned problem of (3), after moving digital music data to an external device the data of the hard disk as delivery origin of data are eliminated -- as (being the so-called --) Although what is necessary is just to create the software of a personal computer so that MUBU [music data] For example, the contents of the hard disk are backed up to another record medium before MUBU, and if the data which backed up after MUBU are restored to a hard disk, the data [MUBU / data] will remain in a hard disk after all.

[0008] (5) When a personal computer moves the digital music data in a hard disk to the device of the exteriors, such as a portable device, in order not to check what kind of device an external instrument is, there is a possibility that digital music data may be passed to an illegal device.

[0009] (6) When passing digital music data to a personal computer, in order not to check what kind of software the software which is controlling the personal computer is from the device of the exteriors, such as a portable device, there is a possibility that digital music data may be passed to illegal software.

[0010] (7) Although it is possible to use ISRC (International Standard Recording Code) contained in music data in order to judge whether two or more music is the same, when dealing with the music data reproduced from CD with a personal computer, there are some which do not contain ISRC data depending on CD. It becomes impossible in this case, to judge whether two or more music is the same.

[0011] (8) Each above function will be able to make the actuation which the implementer of a system does not mean perform, if the software is altered on a personal computer, since control of software realizes.

[0012] This invention is made in view of such a situation, and the music data currently recorded on

the hard disk prevent it being transmitted to the device of the inaccurate exterior and being used for it.

[0013]

[Means for Solving the Problem] When an information processor according to claim 1 transfers the data stored in an are recording means to store data, a maintenance means to hold the conditions of the utilization time of the data stored in the are recording means, and the are recording means to other equipments, Other equipments the data stored in the are recording means with the conditions of the utilization time of the data currently held at the maintenance means based on the judgment result of a judgment means to judge whether the conditions of the utilization time of data can be satisfied, and a judgment means It is characterized by including a transfer means to transfer to other equipments.

[0014] The conditions of the utilization time of data can contain accounting conditions or a copy restriction at the time of a playback restriction and playback.

[0015] When the information processing approach according to claim 3 transfers the data stored by processing of the are recording step which stores data, the maintenance step holding the conditions of the utilization time of the data stored by processing of an are recording step, and an are recording step to other equipments, The judgment step which judges whether other equipments can satisfy the conditions of the utilization time of data, It is characterized by including the transfer step which transfers the data stored by processing of an are recording step to other equipments with the conditions of the utilization time of the data held by processing of a maintenance step based on the judgment result in a judgment step.

[0016] The program of a program storing medium according to claim 4 When transferring the data stored by processing of the are recording step which stores data, the maintenance step holding the conditions of the utilization time of the data stored by processing of an are recording step, and an are recording step to other equipments, The judgment step which judges whether other equipments can satisfy the conditions of the utilization time of data, It is characterized by including the transfer step which transfers the data stored by processing of an are recording step to other equipments with the conditions of the utilization time of the data held by processing of a maintenance step based on the judgment result in a judgment step.

[0017] In an information processor according to claim 1, the information processing approach according to claim 3, and a program storing medium according to claim 4, when transferring the data stored to other equipments, it is judged whether other equipments can satisfy the conditions of the utilization time of data, and data transfer to other equipments with the conditions of the utilization time of data based on the judgment result.

[0018]

[Embodiment of the Invention] Drawing 1 is drawing showing the gestalt of 1 operation of the contents data management system concerning this invention. The personal computer 1 is connected to the network 2 which consists of a Local Area Network or the Internet. With cipher systems, such as DES (Data Encryption Standard), it enciphers and a personal computer 1 is recorded while it changes into the method (for example, ATRAC3 (trademark)) of predetermined compression the

data (contents are called hereafter) of the musical sound read in CD (Compact Disc) which received from the EMD (Electrical Music Distribution) server 4-1 thru/or 4-3, or is mentioned later.

[0019] A personal computer 1 records the data of use conditions in which the use conditions of contents are shown corresponding to the contents currently enciphered and recorded.

[0020] The data of use conditions show the number (number of the so-called PD which can be checked out mentioned later) of a portable device (Portable Device (it is also called PD)) which can use the contents corresponding to the data of the use condition for coincidence, for example. Even when only the number shown in the data of use conditions checks out contents, a personal computer 1 can reproduce the contents.

[0021] Or it is shown that the data of use conditions can be copied. When contents are copied to the portable device 6-1 thru/or 6-3, a personal computer 1 can reproduce the contents currently recorded. The count which the portable device 6-1 of contents thru/or 6-3 can be made to memorize may be restricted. In this case, the count which can be copied does not increase.

[0022] Or the data of use conditions show that it can move to other personal computers etc. After moving contents to the portable device 6-1 thru/or 6-3, it becomes impossible to use the contents which the personal computer 1 is recording (contents are deleted, or it becomes impossible to use use conditions, being changed).

[0023] The detail of the data of use conditions is mentioned later.

[0024] The contents which encipher a personal computer 1 and are recorded with the data (for example, a music name or playback conditions etc.) relevant to contents While making the portable device 6-1 connected memorize through the USB (Universal Serial Bus) cable 7-1 Corresponding to having made the portable device 6-1 memorize, the data of the use conditions corresponding to the contents made to memorize are updated (check-out is called hereafter). The count which can check out the data of the use conditions corresponding to the contents which the personal computer 1 is recording on it more when you check out in a detail is reduced by one. Corresponding contents cannot be checked out when the count which can be checked out is 0.

[0025] A personal computer 1 updates the data of the use conditions corresponding to the contents which made them memorize with the data relevant to contents corresponding to having made the portable device 6-2 memorize while storing the contents currently enciphered and recorded in the portable device 6-2 connected through the USB cable 7-2. A personal computer 1 updates the data of the use conditions corresponding to the contents which made them memorize with the data relevant to contents corresponding to having made the portable device 6-3 memorize while storing the contents currently enciphered and recorded in the portable device 6-3 connected through the USB cable 7-3.

[0026] moreover, the data of the use conditions corresponding to the contents which the personal computer 1 made the portable device 6-1 eliminate the contents which the personal computer 1 checked out to the portable device 6-1 connected through the USB cable 7-1 (or it carries out by the ability not using it -- making), and were made to eliminate are updated (check-in is called hereafter). More, when you check in, the count which can check out the corresponding data of the use conditions of contents which the personal computer 1 is recording is increased by the detail one.

[0027] the data of the use conditions corresponding to the contents which the personal computer 1 made the portable device 6-2 eliminate the contents which the personal computer 1 checked out to the portable device 6-2 connected through the USB cable 7-2 (or it carries out by the ability not using it -- making), and were made to eliminate are updated. the data of the use conditions corresponding to the contents which the personal computer 1 made the portable device 6-3 eliminate the contents which the personal computer 1 checked out to the portable device 6-3 connected through the USB cable 7-3 (or it carries out by the ability not using it -- making), and were made to eliminate are updated.

[0028] Other personal computers which do not illustrate a personal computer 1 cannot check in at the contents checked out to the portable device 6-1. A personal computer 1 cannot check in at the contents which other personal computers checked out to the portable device 6-2. A personal computer 1 cannot check in at the contents which other personal computers checked out to the portable device 6-3.

[0029] When a personal computer 1 starts acquisition of contents from the EMD server 4-1 thru/or 4-3, the EMD registration server 3 transmits the program for connecting with the EMD server 4-1 thru/or 4-3 to a personal computer 1 while transmitting a personal computer 1, the EMD server 4-1, or an authentication key required for the mutual recognition of 4-3 to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1.

[0030] The EMD server 4-1 supplies contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1 with the data (for example, a music name or a playback limit etc.) relevant to contents. The EMD server 4-2 supplies contents to a personal computer 1 with the data relevant to contents through a network 2 corresponding to the demand of a personal computer 1. The EMD server 4-3 supplies contents to a personal computer 1 with the data relevant to contents through a network 2 corresponding to the demand of a personal computer 1.

[0031] The contents which the EMD server 4-1 thru/or each of 4-3 supply are compressed by the same or different compressive method. The contents which the EMD server 4-1 thru/or each of 4-3 supply are enciphered by the same or different method of encryption.

[0032] The WWW (World Wide Web) server 5-1 supplies the data (for example, a music name or a composer name etc.) corresponding to the contents read in CDs (for example, the album name of CD or the selling firm of CD etc.) and CD which read contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1. The WWW server 5-2 supplies the data corresponding to the contents read in CD and CD which read contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1.

[0033] The portable device 6-1 memorizes the contents (namely, checked-out contents) supplied from the personal computer 1 with the data (for example, a music name or a playback limit etc.) relevant to contents. Based on the data relevant to contents, the portable device 6-1 is reproduced and outputs the memorized contents to the headphone which are not illustrated.

[0034] For example, when it is going to reproduce exceeding the count of playback as a playback limit memorized as data relevant to contents, the portable device 6-1 suspends playback of

corresponding contents. When it is going to reproduce after passing over the playback term as a playback limit memorized as data relevant to contents, the portable device 6-1 suspends playback of corresponding contents.

[0035] A user can reproduce the memorized contents which removed the portable device 6-1 which memorized contents from the personal computer 1, and walked around with, and can listen to the music corresponding to contents etc. by headphone etc.

[0036] The portable device 6-2 memorizes the contents supplied from the personal computer 1 with the data relevant to contents. Based on the data relevant to contents, the portable device 6-2 is reproduced and outputs the memorized contents to the headphone which are not illustrated. A user can reproduce the memorized contents which removed the portable device 6-2 which memorized contents from the personal computer 1, and walked around with, and can listen to the music corresponding to contents etc. by headphone etc.

[0037] The portable device 6-3 memorizes the contents supplied from the personal computer 1 with the data relevant to contents. Based on the data relevant to contents, the portable device 6-3 is reproduced and outputs the memorized contents to the headphone which are not illustrated. A user can reproduce the memorized contents which removed the portable device 6-3 which memorized contents from the personal computer 1, and walked around with, and can listen to the music corresponding to contents etc. by headphone etc.

[0038] Hereafter, when it is not necessary to distinguish the portable device 6-1 thru/or 6-3 separately, the portable device 6 is only called.

[0039] Drawing 2 is drawing explaining the configuration of a personal computer 1. CPU (CentralProcessing Unit)11 actually performs various application programs (for details, it mentions later) and OS (Operating System). Generally ROM (Read-only Memory)12 stores the data of immobilization fundamentally of the parameters the program which CPU11 uses, and for an operation. RAM (Random-Access Memory)13 stores a variable parameter suitably in the program used in activation of CPU11, and its activation. These are mutually connected by the host bus 14 which consists of CPU buses etc.

[0040] The host bus 14 is connected to the external buses 16, such as a PCI (Peripheral Component Interconnect/Interface) bus, through the bridge 15.

[0041] A keyboard 18 is operated by the user when inputting various kinds of commands into CPU11. A mouse 19 is operated by the user when performing the directions and selection of the point on the screen of a display 20. A display 20 consists of a liquid crystal display or CRT (Cathode Ray Tube), and displays various information in a text or an image. HDD (Hard Disk Drive)21 drives a hard disk, and records or reproduces the program and information which are performed by CPU11 to them.

[0042] Drive 22 reads the data or the program currently recorded on the magnetic disk 41 with which it is equipped, an optical disk 42 (CD is included), a magneto-optic disk 43, or semiconductor memory 44, and supplies the data or program to RAM13 with which it connects through the interface 17, the external bus 16, the bridge 15, and the host bus 14.

[0043] The portable device 6-1 is connected to the USB port 23-1 through the USB cable 7-1. The

USB port 23-1 outputs the data (for example, the command of contents or the portable device 6-1 etc. is included) supplied from HDD21, CPU11, or RAM13 to the portable device 6-1 through an interface 17, an external bus 16, a bridge 15, or the host bus 14.

[0044] The portable device 6-2 is connected to the USB port 23-2 through the USB cable 7-2. The USB port 23-2 outputs the data (for example, the command of contents or the portable device 6-2 etc. is included) supplied from HDD21, CPU11, or RAM13 to the portable device 6-2 through an interface 17, an external bus 16, a bridge 15, or the host bus 14.

[0045] The portable device 6-3 is connected to the USB port 23-3 through the USB cable 7-3. The USB port 23-3 outputs the data (for example, the command of contents or the portable device 6-3 etc. is included) supplied from HDD21, CPU11, or RAM13 to the portable device 6-3 through an interface 17, an external bus 16, a bridge 15, or the host bus 14.

[0046] The voice-input/output interface 24 which has IEC(International Electrotechnical Commission) 60958 terminal 24a performs interface processing of digitized voice I/O or an analog voice input/output. A loudspeaker 45 outputs the predetermined voice corresponding to contents based on the sound signal supplied from the voice-input/output interface 24.

[0047] These keyboards 18 thru/or the voice-input/output interface 24 are connected to the interface 17, and the interface 17 is connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.

[0048] A network 2 is connected and the communications department 25 stores in the packet of a predetermined method the data (for example, the demand of registration or the Request to Send of contents etc.) supplied from CPU11 or HDD21. While transmitting through a network 2, the data (for example, an authentication key or contents etc.) stored in the packet which received are outputted to CPU11, RAM13, or HDD21 through a network 2.

[0049] Formed in one as a semiconductor IC, CPU32 of the adapter 26 with which a personal computer 1 is equipped has two incomes with CPU11 of a personal computer 1 through an external bus 16, a bridge 15, and the host bus 14, and performs various kinds of processings. CPU32 performs various kinds of processings upwards, and RAM33 memorizes required data and a required program. Nonvolatile memory 34 memorizes the data which need to be held even after the power source of a personal computer 1 is turned off. When the program enciphered has been transmitted to ROM36 from the personal computer 1, the program which decodes it is memorized. RTC (Real Time Clock)35 -- a time check -- actuation is performed and time information is offered.

[0050] The communications department 25 and an adapter 26 are connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.

[0051] Hereafter, when it is not necessary to distinguish the USB port 23-1 thru/or 23-3 separately, the USB port 23 is only called. Hereafter, when it is not necessary to distinguish the USB cable 7-1 thru/or 7-3 separately, the USB cable 7 is only called.

[0052] Next, the configuration of the portable device 6 is explained with reference to drawing 3. A power circuit 52 makes the portable device 6 whole drive by transforming into the internal power of a predetermined electrical potential difference the supply voltage supplied from a dry cell 51, and supplying CPU53 thru/or a display 67.

[0053] The USB controller 57 supplies the data containing the contents transmitted from the personal computer 1 to CPU53 through an internal bus 58, when it connects with a personal computer 1 through the USB cable 7 through the USB connector 56.

[0054] The data transmitted from a personal computer 1 consist of 64 bytes per one packet of data, and are transmitted from a personal computer 1 at the transfer rate of 12 Mbit/sec.

[0055] The data transmitted to the portable device 6 consist of a header and contents. While content ID, a file name, header size, a contents key, a file size, Codec ID, file information, etc. are stored, playback limit data required for playback limit processing, initiation time, termination time, the count limit, the count counter of playback, etc. are stored in the header. Contents are encoded and enciphered by coding methods, such as ATRAC3.

[0056] Header size expresses the data lengths (for example, 33 etc. bytes etc.) of a header, and a file size expresses the data lengths (for example, 33,636,138 etc. bytes etc.) of contents.

[0057] A contents key is a key for decoding the contents enciphered, and is transmitted to the portable device 6 from a personal computer 1 in the condition of having been enciphered based on the session key (momentary key) generated by processing of the mutual recognition of a personal computer 1 and the portable device 6.

[0058] When the portable device 6 is connected to the USB port 23 of a personal computer 1 through the USB cable 7, the portable device 6 and a personal computer 1 perform processing of mutual recognition. Processing of this mutual recognition is processing of authentication of for example, a challenge response method. Incidentally, DSP59 of the portable device 6 performs processing of decryption (decode), when processing authentication of a challenge response method.

[0059] A challenge response method is a method which answers with the value (response) which the portable device 6 generated to a certain value (challenge) which a personal computer 1 generates using the private key currently shared with a personal computer 1. Since the value which a personal computer 1 generates changes for every processing of authentication in processing of the mutual recognition of a challenge response method each time, even if the value which the portable device 6 outputted and which was generated using the private key is read for example, and it receives the so-called attack of spoofing, since the values used for mutual recognition differ, by processing of the following mutual recognition, as for a personal computer 1, injustice is detectable.

[0060] Content ID is ID for specifying contents corresponding to contents.

[0061] Codec ID is ID corresponding to the coding method of contents, for example, codec ID"1" corresponds to ATRAC3, and codec ID"0" corresponds to MP3 (MPEG (MovingPicture Experts Group) Audio Layer-3).

[0062] A file name is data which changed into the ASCII (American National Standard Codefor Information Interchange) code the contents file (it mentions later) which the personal computer 1 corresponding to contents is recording, and file information is data which changed the music name corresponding to contents, the artist name, the songwriter name, or the composer name into the ASCII code.

[0063] Playback limit data are data in which it is shown whether the period (namely, initiation time or termination time) which can reproduce contents, or the count limit (limit which is a reproductive

count) is set up. When the count limit is set up, "1" is assigned, when the reproducible period is set up, "2" is assigned, and "0" is assigned to playback limit data when all periods in which a count limit and playback are possible are not set up (when purchased by the so-called acquisition).

[0064] Initiation time and termination time are data in which the range of a refreshable period is shown, when playback limit data are "2." For example, when initiation time is "00040F" and termination time is "00070F", corresponding contents can be reproduced from April 15, 2000 to July 15, 2000.

[0065] Similarly, when the playback limit data of a count limit and the count counter of playback are "1" or "2", a count limit is the refreshable count beforehand set up corresponding to the contents, and the count counter of playback shows the count which is updated by CPU53 and by which contents were reproduced, when processing of playback of the contents is performed. For example, when the refreshable count of the contents is 2 times when a count limit is "02", and the count counter of playback is "01", the count by which the contents were reproduced is 1 time.

[0066] For example, initiation time is "00040F", playback limit data are "2", termination time is "00070F", and when a count limit is "02", the portable device 6 can reproduce corresponding contents [a bis die every] in the periods from April 15, 2000 to July 15, 2000.

[0067] For example, when playback limit data are "1", initiation time is "000000", termination time is "000000", a count limit is "0a" and the count counter of playback is "05", corresponding contents do not have a limit of a refreshable period, a refreshable count is 10 times, and the reproduced count is 5 times.

[0068] When the portable device 6 receives the write-in instruction of contents with contents from a personal computer 1, CPU53 which performs the main program read from ROM55 to RAM54 makes the contents which controlled reception and the flash memory controller 60 and received the write-in instruction from the personal computer 1 write in a flash memory 61.

[0069] A flash memory 61 has the storage capacity of about 64 MByte(s), and memorizes contents. Moreover, the code for playback for elongating the contents compressed by the predetermined compression method is beforehand stored in the flash memory 61.

[0070] In addition, a flash memory 61 can be made removable as a memory card at the portable device 6.

[0071] When the playback instruction corresponding to depression actuation of the playback/earth switch which is not illustrated by the user is supplied to CPU53 through the actuation key controller 62, CPU53 makes the flash memory controller 60 read the code for playback, and contents, and DSP59 is made to transmit it to it from a flash memory 61.

[0072] It reproduces and DSP59 supplies the reproduced data (D1 shows in drawing 3) to the digital to analog circuit 63, after carrying out error detection for contents by the CRC (Cyclic Redundancy Check) method based on the code for playback transmitted from the flash memory 61.

[0073] While DSP59 reproduces contents based on the master clock MCLK from dispatch child 59A which changes with Xtal by which was constituted by one and external was carried out to it with the dispatch circuit which was established in the interior, and which is not illustrated The bit clock BCLK of the predetermined frequency generated based on the master clock MCLK and the master

clock MCLK in the internal oscillator circuit. The clock LRCLK of operation which becomes a list from the L channel clock LCLK of a frame unit and the R channel clock RCLK is supplied to the digital-to-analog conversion circuit 63.

[0074] When supplying an above-mentioned clock of operation to the digital-to-analog conversion circuit 63 according to the code for playback when reproducing contents, and not reproducing contents, DSP59 suspends supply of a clock of operation according to the code for playback, stops the digital-to-analog conversion circuit 63, and reduces the consumed electric power of the portable device 6 whole.

[0075] Similarly, external [of the radiators 53A or 57A which CPU53 and the USB controller 57 also become with Xtal] is carried out, respectively, and they perform predetermined processing based on the master clock MCLK supplied from Radiators 53A or 57A, respectively.

[0076] Thus, with constituting, the clock generation module for performing clock supply to each circuit block of CPU53, DSP59, and USB controller 57 grade becomes unnecessary, and the portable device 6 can be miniaturized while simplifying circuitry.

[0077] The digital-to-analog conversion circuit 63 changes the reproduced contents into the sound signal of an analog, and supplies this to an amplifying circuit 64. An amplifying circuit 64 amplifies a sound signal and supplies a sound signal to the headphone which are not illustrated through the headphone jack 65.

[0078] Thus, the portable device 6 suspends playback of contents, when press actuation of playback/the earth switch is carried out during playback, while reproducing the contents memorized by the flash memory 61 based on control of CPU53, when press actuation of the playback/the earth switch which is not illustrated is carried out.

[0079] The portable device 6 resumes playback of contents from the location stopped based on control of CPU53, when press actuation of playback/the earth switch is again carried out after a halt. When it passes for several seconds, without playback/earth switch suspending playback by press actuation, and adding actuation, the portable device 6 turns off a power source automatically, and reduces power consumption.

[0080] Incidentally, when press actuation of playback/the earth switch is carried out after the power source became off, the portable device 6 does not reproduce contents from the location which last time stopped, but reproduces them from the 1st music.

[0081] moreover, CPU53 of the portable device 6 -- the LCD controller 68 -- controlling -- a display 67 -- the condition of a playback mode, equalizer adjustments (for example, repeat playback, intro playback, etc.) (namely, adjustment of the gain corresponding to the frequency band of a sound signal), a tune number number, performance time amount, playback, a halt, and a rapid traverse -- information, such as conditions, such as return, sound volume, and a residue of a dry cell 51, is already displayed.

[0082] Furthermore, the portable device 6 stores the so-called FAT (File Allocation Table), such as a block location of a flash memory 61 where the number of the contents currently written in the flash memory 80 and each contents are written in EEPROM68, and various memory are recording information in addition to this.

[0083] Incidentally, in the gestalt of this operation, contents are treated considering 64KByte as 1 block, and the block location corresponding to the contents of one music is stored in FAT.

[0084] If the block location corresponding to the contents of the 1st music will be written in a flash memory 61 as FAT if the contents of the 1st music are written in a flash memory 61 by control of CPU53, next the contents of the 2nd music are written in a flash memory 61 when FAT is stored in a flash memory 61 for example, the block location corresponding to the contents of the 2nd music will be written in a flash memory 61 (the same field as the 1st music) as FAT.

[0085] Thus, FAT is rewritten at every writing of the contents to a flash memory 61, and the same data are further written in reserve at a duplex for protection of data.

[0086] If FAT is written in a flash memory 61, since the same field of a flash memory 61 will be rewritten twice corresponding to one writing of contents, by the count of little writing of contents, the count of rewriting specified to the flash memory 61 will be become, and rewriting of a flash memory 61 will become impossible.

[0087] Then, the portable device 6 makes EEPROM68 memorize FAT, and lessens the frequency of rewriting of the flash memory 61 corresponding to one writing of contents.

[0088] By making EEPROM68 memorize FAT with many counts of rewriting, the portable device 6 can increase the count which can do the writing of contents to dozens or more times as compared with the case where a flash memory 61 is made to memorize FAT. Furthermore, since CPU53 is made to write in so that FAT may be added to EEPROM68, it prevents lessening the frequency of rewriting of the same field of EEPROM68, and EEPROM68 rewriting for a short period of time, and becoming impossible.

[0089] The portable device 6 recognizes that USB connection was made based on the interrupt signal supplied to CPU53 from the USB controller 57, when it connects with a personal computer 1 through the USB cable 7 (this is hereafter called USB connection).

[0090] The portable device 6 controls a power circuit 52, and stops supply of the power from a dry cell 51 while it will receive supply of the external power of a convention current value from a personal computer 1 through the USB cable 7, if it recognizes that USB connection was made.

[0091] CPU53 stops processing of playback of the contents of DSP59, when USB connection is made. Thereby, CPU53 prevents that the external power supplied from a personal computer 1 exceeds a convention current value, and controls it to be always able to receive the external power of a convention current value.

[0092] Thus, if USB connection is made, since CPU53 will be switched to the power supplied from a personal computer 1 from the power supplied from a dry cell 51, the external power from the personal computer 1 with a cheap power unit price is used, the power consumption of the dry cell 51 with a high power unit price is reduced, and it can prolong the life of a dry cell 51 in this way.

[0093] In addition, when supply of external power is received from a personal computer 1 through the USB cable 7, by stopping regeneration of DSP59, CPU53 reduces the radiation from DSP59, and reduces much more radiation of the whole system which contains a personal computer 1 as the result.

[0094] Drawing 4 is a block diagram explaining the configuration of the function of a personal

computer 1 realized by the predetermined program execution of CPU11 etc. The contents manager 111 consists of two or more programs, such as the EMD selection program 131, check-in/check-out manager 132, the cipher system conversion program 135, the compression method conversion program 136, the encryption program 137, the use condition conversion program 139, the use condition manager 140, the authentication program 141, the decode program 142, the driver 143 for PD, the program 144 for purchase, and the program 145 for purchase.

[0095] the contents manager 111 -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the contents manager 111 directly) -- it is constituted like.

[0096] When the contents manager 111 is installed in a personal computer 1, the EMD selection program 131 is not included in the contents manager 111, but is received from the EMD registration server 3 through a network 2 in processing of the registration of EMD mentioned later. The EMD selection program 131 chooses connection with the EMD server 4-1 thru/or either of 4-3, and makes the application 115 for purchase, the program 144 for purchase, or 142 perform the communication links (for example, download of contents when purchasing contents etc.) with the EMD server 4-1 thru/or either of 4-3.

[0097] Check-in/check-out manager 132 checks in at the contents which check out the contents stored in the contents file 161-1 thru/or 161-N based on the use condition file 162-1 thru/or 162-N currently recorded on check-in or a setup of check-out, and the contents database 114 to the portable device 6-1 thru/or either of 6-3, or are memorized by the portable device 6-1 thru/or 6-3.

[0098] Check-in/check-out manager 132 updates the data of the use conditions stored in the use condition file 162-1 thru/or 162-N currently recorded on the contents database 114 corresponding to processing of check-in or check-out.

[0099] The copy manager 133 copies the contents stored in the contents file 161-1 thru/or 161-N based on the use condition file 162-1 thru/or 162-N currently recorded on the contents database 114 to the portable device 6-1 thru/or either of 6-3, or copies contents to the contents database 114 from the portable device 6-1 thru/or 6-3.

[0100] The migration manager 134 moves the contents stored in the contents file 161-1 thru/or 161-N based on the use condition file 162-1 thru/or 162-N currently recorded on the contents database 114 to the portable device 6-1 thru/or either of 6-3, or moves contents to the contents database 114 from the portable device 6-1 thru/or 6-3.

[0101] The method of encryption of contents with which the application program 115 for purchase received the cipher system conversion program 135 from the EMD server 4-1 through the network 2, The method of encryption of the contents which the program 144 for purchase received from the EMD server 4-2, Or the method of encryption of the contents which the program 145 for purchase received from the EMD server 4-3 is transformed into the method of the same encryption as the contents stored in the contents file 161-1 thru/or 161-N which the contents database 114 is recording.

[0102] Moreover, the cipher system conversion program 135 changes the contents to check out into

the portable device 6-1 or a cipher system with available 6-3, when you check out contents to the portable device 6-1 or 6-3.

[0103] The method of compression of contents with which the application program 115 for purchase received the compression method conversion program 136 from the EMD server 4-1 through the network 2, The method of compression of the contents which the program 144 for purchase received from the EMD server 4-2, Or the method of compression of the contents which the program 145 for purchase received from the EMD server 4-3 is transformed into the method of the same compression as the contents stored in the contents file 161-1 thru/or 161-N which the contents database 114 is recording.

[0104] Moreover, the compression method conversion program 136 changes the contents to check out into the portable device 6-1 or the method of compression with available 6-3, when you check out contents to the portable device 6-1 or 6-3.

[0105] It is read in CD and the encryption program 137 is enciphered by the method of the same encryption as the contents stored in the contents file 161-1 whose contents database 114 is recording the contents (not enciphered) supplied from the sound recording program 113 thru/or 161-N.

[0106] It is read in CD and compression/elongation program 138 is encoded by the method of the same coding as the contents stored in the contents file 161-1 whose contents database 114 is recording the contents (not compressed) supplied from the sound recording program 113 thru/or 161-N. Compression/elongation program 138 elongates the contents encoded (decode).

[0107] the data (being the so-called --) which, as for the use condition conversion program 139, the application program 115 for purchase shows the use conditions of the contents which received from the EMD server 4-1 through a network 2 Usage Rule, the data in which the use conditions of the contents which the program 144 for purchase received from the EMD server 4-2 are shown, Or the data in which the use conditions of the contents which the program 145 for purchase received from the EMD server 4-3 are shown are changed into the same format as the use condition data stored in the use condition file 162-1 thru/or 162-N which the contents database 114 is recording.

[0108] Moreover, the use condition conversion program 139 changes the data of the use conditions corresponding to the contents to check out into the data of the portable device 6-1 or use conditions with available 6-3, when you check out contents to the portable device 6-1 or 6-3.

[0109] The use condition manager 140 detects the alteration of the data of use conditions based on the hash value (it mentions later) corresponding to the data of the use conditions stored in the use condition file 162-1 thru/or 162-N currently recorded on the contents database 114, before performing processing of the copy of contents, migration, check-in, or check-out. The use condition manager 140 updates the hash value corresponding to the data of use conditions for the data of the use conditions stored in the use condition file 162-1 thru/or 162-N accompanying processing of the copy of contents, migration, check-in, or check-out currently recorded on the contents database 114 corresponding to updating.

[0110] The authentication program 141 performs processing of the mutual recognition of the contents manager 111 and the application program 115 for purchase, and processing of the mutual

recognition of the contents manager 111 and the program 144 for purchase. Moreover, the authentication program 141 has memorized the authentication key used by processing of the mutual recognition of the EMD server 4-1 and the application program 115 for purchase, processing of the mutual recognition of the EMD server 4-2 and the program 144 for purchase, and processing of the mutual recognition of the EMD server 4-3 and the program 145 for purchase.

[0111] The authentication key which the authentication program 141 uses by processing of mutual recognition is not memorized by the authentication program 141 when the contents manager 111 is installed in a personal computer 1, but when processing of registration is normally performed by the display operator guidance program 112, is supplied from the EMD registration server 3, and is memorized by the authentication program 141.

[0112] The decode program 142 decodes contents, when a personal computer 1 reproduces the contents stored in the contents file 161-1 thru/or 161-N which the contents database 114 is recording.

[0113] The driver 143 for PD supplies the command which makes the portable device 6-2 perform predetermined processing to contents or the portable device 6-2, when you check out predetermined contents to the portable device 6-2, or when you check in at predetermined contents from the portable device 6-2.

[0114] The driver 143 for PD supplies the command which performs predetermined processing to contents or a device driver 116-1 to a device driver 116-1, when you check out predetermined contents to the portable device 6-1, or when you check in at predetermined contents from the portable device 6-1.

[0115] The driver 143 for PD supplies the command which performs predetermined processing to contents or a device driver 116-2 to a device driver 116-2, when you check out predetermined contents to the portable device 6-3, or when you check in at predetermined contents from the portable device 6-3.

[0116] It is the so-called plug-in program, and the program 144 for purchase is installed with the contents manager 111, is supplied through a network 2 from the EMD registration server 3, or it is recorded on predetermined CD and supplied. The program 144 for purchase transmits and receives the contents manager 111 and data through the interface of the predetermined format which the contents manager 111 has, when installed in a personal computer 1.

[0117] the program 144 for purchase -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the program 144 for purchase directly) -- it is constituted like.

[0118] The program 144 for purchase receives contents from the EMD server 4-2 while requiring transmission of predetermined contents of the EMD server 4-2 through a network 2. Moreover, the program 144 for purchase performs processing of accounting, when receiving contents from the EMD server 4-2.

[0119] The program 145 for purchase is a program installed with the contents manager 111, and it

receives contents from the EMD server 4-3 while it requires transmission of predetermined contents of the EMD server 4-3 through a network 2. Moreover, the program 145 for purchase performs processing of accounting, when receiving contents from the EMD server 4-3.

[0120] The display operator guidance program 112 displays the image of a predetermined window on a display 20 based on the filtering data file 181, the display data file 182, an image file 183-1, 183-K, or the hysteresis data file 184, and directs activation of processings, such as check-in or check-out, based on the actuation to a keyboard 18 or a mouse 19 at the contents manager 111.

[0121] The filtering data file 181 stores the data for making weighting each contents stored in the contents file 161-1 thru/or 161-N currently recorded on the contents database 114, and is recorded on HDD21.

[0122] The display data file 182 stores the data corresponding to the contents stored in the contents file 161-1 thru/or 161-N currently recorded on the contents database 114, and is recorded on HDD21.

[0123] An image file 183-1 thru/or 183-K store the image corresponding to the contents file 161-1 thru/or 161-N currently recorded on the contents database 114, or the image corresponding to the package mentioned later, and is recorded on HDD21.

[0124] Hereafter, when it is not necessary to distinguish an image file 183-1 thru/or 183-K separately, an image file 183 is only called.

[0125] The contents stored in the contents file 161-1 thru/or 161-N currently recorded on the contents database 114 store historical data, such as a checked-out count, a count at which he checked in, and its date, and the hysteresis data file 184 is recorded on HDD21.

[0126] The display operator guidance program 112 receives the key for authentication, and the EMD selection program 131 from the EMD registration server 3, and supplies the key for authentication, and the EMD selection program 131 to the contents manager 111 while it transmits ID of the contents manager 111 beforehand memorized to the EMD registration server 3 through a network 2 at the time of processing of registration.

[0127] The sound recording program 113 displays the image of a predetermined window, and reads data, such as sound recording time amount of contents, from CD which is the optical disk 42 with which the drive 22 was equipped based on the actuation to a keyboard 18 or a mouse 19.

[0128] The sound recording program 113 minds a network 2 based on the sound recording time amount of the contents currently recorded on CD etc. While requiring transmission of the data (for example, music name etc.) corresponding to the contents currently recorded on the WWW server 5-1 or 5-2 by the data (for example, an album name or an artist name etc.) or CD corresponding to CD. The data corresponding to the contents currently recorded on the data or CD corresponding to CD from the WWW server 5-1 or 5-2 are received.

[0129] The sound recording program 113 supplies the data corresponding to the contents currently recorded on the data or CD corresponding to received CD to the display operator guidance program 112.

[0130] Moreover, when directions of sound recording are inputted, the sound recording program 113 reads contents from CD which is the optical disk 42 with which the drive 22 was equipped, and outputs them to the contents manager 111.

[0131] The contents which the contents database 114 is compressed by the predetermined method supplied from the contents manager 111, and are enciphered by the predetermined method are stored in either the contents file 161-1 thru/or 161-N (it records on HDD21). The contents database 114 is stored in either the contents file 161-1 for which the data of the use conditions corresponding to the contents stored in the contents file 161-1 thru/or 161-N, respectively are stored in contents the use condition file 162-1 respectively corresponding to 161-N thru/or 162-N (it records on HDD21).

[0132] The contents database 114 may record the contents file 161-1 thru/or 161-N or the use condition file 162-1 thru/or 162-N as a record.

[0133] For example, the data of the use conditions corresponding to the contents stored in the contents file 161-1 are stored in the use condition file 162-1. The data of the use conditions corresponding to the contents stored in contents file 161-N are stored in use condition file 162-N.

[0134] In addition, the data currently recorded on the use condition file 162-1 thru/or 162-N are equivalent to the data currently recorded on the term database mentioned later, or the data currently recorded on the music database. That is, the contents database 114 includes the term database and music database which are mentioned later, and is constituted.

[0135] Hereafter, when it is not necessary to distinguish the contents file 161-1 thru/or 161-N separately, the contents file 161 is only called. Hereafter, when it is not necessary to distinguish the use condition file 162-1 thru/or 162-N separately, the use condition file 162 is only called.

[0136] The application program 115 for purchase is supplied through a network 2 from the EMD registration server 3, or is recorded and supplied to predetermined CD-ROM. The application program 115 for purchase receives contents from the EMD server 4-1, and supplies them to the contents manager 111 while it requires transmission of predetermined contents of the EMD server 4-1 through a network 2. Moreover, the application program 115 for purchase performs processing of accounting, when receiving contents from the EMD server 4-1.

[0137] Next, matching with the contents file 161-1 thru/or 161-N stored in the data stored in the display data file 82 and a contents database is explained.

[0138] The contents stored in either the contents file 161-1 thru/or 161-N belong to a predetermined package. A package is either an original package and my selection package or a filtering package more at a detail.

[0139] One or more contents belong and an original package is equivalent to the classification (for example, it corresponds to the so-called album) of the EMD server 4-1 thru/or the contents in 4-3, or CD of one sheet. Contents cannot belong to one of original packages, and cannot belong to two or more original packages. Moreover, the original package with which contents belong cannot be changed. A user can edit a part of information corresponding to an original package (modification of the information which information added or added).

[0140] One or more contents from which the user chose the my selection package as arbitration belong. A user can edit into arbitration whether which contents belong to a my selection package. Contents can belong to one or more my selection packages at coincidence. Moreover, contents do not need to belong to which my selection package.

[0141] The contents chosen based on the filtering data stored in the filtering data file 181 belong to a filtering package. Filtering data are supplied through a network 2 from the EMD server 4-1 thru/or 4-3, the WWW server 5-1, 5-2, etc., or are recorded on predetermined CD and supplied. A user can edit the filtering data stored in the filtering data file 181.

[0142] Filtering data serve as criteria which choose predetermined contents or compute the weight corresponding to contents. For example, if the filtering data corresponding to the J-POP (pop of Japan) top ten of this week are used, a personal computer 1 can specify the contents of the 1st place of the pop of Japan of this week thru/or the contents of the 10th place of the pop of Japan of this week.

[0143] The filtering data file 181 contains the filtering data with which the period checked out in January [past] chooses contents as long order, the filtering data which choose contents with many counts checked out at past half a year, or the filtering data which chooses the contents by which the alphabetic character of "love" is contained in the music name.

[0144] Thus, the contents of a filtering package make the indicative data 221 (the data which the user set as the indicative data 221 for contents are included) for contents corresponding to contents or historical data 184, and filtering data correspond, and are chosen.

[0145] A driver 117 outputs the analog signal corresponding to the contents which drove the voice-input/output interface 24 on the radical of control, such as the contents manager 111, and outputted to it the contents which inputted the contents which are digital data supplied from the outside, and supplied the contents manager 111, or were supplied from the contents database 114 through the contents manager 111 as digital data, or were supplied to it from the contents database 114 through the contents manager 111.

[0146] Drawing 5 is drawing showing the example of the display operator guidance window which the operator guidance program 112 displays on a display 20, when starting the display operator guidance program 112.

[0147] In order to edit the carbon button 203 for displaying the field which sets up processing of the carbon button 202 for making a display operator guidance window start the carbon button 201 for starting the sound recording program 113, and the EMD selection program 131, check-in, or check-out, and a my selection package, the carbon button 204 grade for displaying the field is arranged.

[0148] When the carbon button 205 is chosen, the data corresponding to an original package are displayed on the field 211. When the carbon button 206 is chosen, the data corresponding to a my selection package are displayed on the field 211. When the carbon button 207 is chosen, the data corresponding to a filtering package are displayed on the field 211.

[0149] The data displayed on the field 211 are data about a package, for example, are a package name or an artist name.

[0150] for example, -- drawing 5 -- setting -- a package -- a name -- " -- the first -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- and -- a package -- a name -- " -- second -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- etc. -- the field -- 211 -- displaying -- having .

[0151] The data corresponding to the contents belonging to the package chosen in the field 211 are

displayed on the field 212. The data displayed on the field 212 are for example, a music name, performance time amount, or the count that can be checked out.

[0152] For example, in drawing 5 , since the package corresponding to package name "second" is chosen Bar" and the count which can be checked out of package name "music name corresponding to contents belonging to package corresponding to second"" south (for example, one of the eighth notes is equivalent to one check-out, and an eighth note shows two check-out by two), and a list -- a music name -- "a north graveyard", the count (an eighth note shows one check-out by one) which can be checked out are displayed on the field 212.

[0153] Thus, it is shown that corresponding contents can check out once one eighth note as a count which is displayed on the field 212 and which can be checked out.

[0154] The rest as a count which is displayed on the field 212 and which can be checked out cannot check out corresponding contents (the count which can be checked out is 0.). (-- however, a personal computer 1 can reproduce the contents.) -- things are shown. Moreover, the G clef as a count which is displayed on the field 212 and which can be checked out shows what no limit is in the count of check-out of corresponding contents (he can check out any number of times).

[0155] In addition, as shown in drawing 5 , it not only displays the count which can be checked out by the number of predetermined graphic forms (for example, a circle, a star, the moon, etc. are sufficient), but you may display it in a figure etc.

[0156] Moreover, the field 208 which displays the image matched with the package or contents chosen on a display operator guidance window (it corresponds to the image file 183-1 of drawing 4 thru/or either of the 183-K) is arranged. A carbon button 209 is clicked when reproducing the contents chosen (the voice corresponding to contents is made to output to a loudspeaker 45).

[0157] When a carbon button 205 is chosen and the data corresponding to an original package are displayed on the field 211, and choosing the music name of the predetermined contents currently displayed on the field 212 and operating elimination, the display operator guidance program 112 makes the predetermined contents stored in the contents database 114 corresponding to the music name chosen as the contents manager 111 eliminate.

[0158] When the carbon button (carbon button 255 mentioned later) of the window which the sound-recording program 113 displays is chosen, it is (activated) and the contents read from CD are recorded on the contents database 114, the display operator-guidance program 112 displays the field 213 which displays the music name of the contents memorized by the portable device 6-1 beforehand specified as the display operator-guidance window thru/or either of 6-3.

[0159] When the carbon button of the window which the sound recording program 113 displays is chosen and the contents read from CD are recorded on the contents database 114, the display operator guidance program 112 makes the portable device 6-1 specified beforehand thru/or either of 6-3 check out the contents which were recorded on the contents database 114 at the contents manager 111 and which were read from CD.

[0160] The music name of contents is made to correspond to the field 213, and the notation which shows whether the contents can check in at a personal computer 1 is displayed on the leftmost of the field 213. For example, "O" located in the leftmost of the field 213 shows what (that is, the

personal computer 1 was checked out) the contents corresponding to the music name of contents can check in at a personal computer 1. "x" located in the leftmost of the field 213 shows what (that is, a personal computer 1 is not checked out, for example, other personal computers were checked out) the contents corresponding to the music name of contents cannot check in at a personal computer 1.

[0161] When the display operator guidance program 112 displays the field 213 on a display operator guidance window, the display operator guidance program 112 In a display operator guidance window The name of the portable package (par cage with which the contents memorized by the portable device 6-1 thru/or either of 6-3 belong) with which the contents memorized by the portable device 6-1 specified beforehand thru/or either of 6-3 belong The carbon button 215 which performs the carbon button 210 and check-in, or check-out for closing the field 214 and the field 213 to display is displayed.

[0162] When the display operator guidance program 112 displays the field 213 on a display operator guidance window, furthermore, the display operator guidance program 112 In a display operator guidance window The carbon button 216 which sets up check-out of the contents corresponding to the music name chosen in the field 212, A setup of the carbon button 217 which sets up check-in of the contents corresponding to the music name chosen in the field 213, the carbon button 218 which sets up check-in of all the contents corresponding to the contents name displayed on the field 213 and check-in, or check-out The carbon button 219 to cancel is arranged.

[0163] Only by setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, a personal computer 1 does not perform processing of check-in or check-out.

[0164] When a carbon button 215 is clicked after carrying out a setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, the display operator guidance program 112 makes the contents manager 111 perform processing of check-in or check-out. When a carbon button 215 is clicked, namely, the display operator guidance program 112 It is based on a setup of check-in or check-out. To the contents manager 111 [whether contents are made to transmit to the portable device 6-1 thru/or either of 6-3, and] Or while making the predetermined commands (for example, command which makes the predetermined contents which the portable device 6-1 thru/or either of 6-3 have memorized eliminate) corresponding to check-in transmit The data of the use conditions stored in the use condition file 162 corresponding to the transmitted contents or the command are made to update.

[0165] When check-in or check-out is performed, the display operator guidance program 112 updates the historical data stored in the hysteresis data file 184 corresponding to the contents which transmitted, or the transmitted command. Historical data consist of the information which specifies the contents checked in or checked out or the date checked in or checked out in the contents, the portable device 6-1 with which he was checked out in the contents, or the name of 6-3.

[0166] Since processing of a setup of check-in or check-out can be performed in a short time, a user can know quickly the condition after check-in or activation of processing of check-out, the count of processing of the check-in which time amount requires, or check-out can be reduced, and the whole (a setup and activation are contained) time amount required for check-in or check-out can be shortened.

[0167] Drawing 6 is drawing explaining the example of the window which the sound recording program 113 displays on a display 20. For example, the sound recording program 113 displays the title of CDs, such as "ASHINKURONAIZUDO", on the field 251 based on the information on CD received from the WWW server 5-2. Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays artist names, such as an "arrowhead", on the field 252.

[0168] Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays music names, such as "heat", a "planet", "black", and "Seoul", on the part which displays the music name of the field 253. Similarly, the sound recording program 113 displays artist names, such as an "arrowhead", on the part which displays the artist of the field 253.

[0169] After the sound recording program 113 receives the information on predetermined CD, the sound recording program 113 stores the information on CD in the predetermined directory of HDD21.

[0170] When a carbon button 254 etc. is clicked and directions of acquisition of the information on CD are received, as for the sound recording program 113, the predetermined directory of HDD21 is searched first. The sound recording program 113 makes it choose whether the dialog box which is not illustrated is displayed and the information on CD stored in the user to the directory is used, when the information on CD is stored in the directory.

[0171] When the carbon button 256 which directs initiation of the sound recording of the contents arranged in the window which the sound recording program 113 displays is clicked, the sound recording program 113 supplies the contents which read contents from CD stored in the drive 22, and were read from CD to the contents manager 111 with the information on CD. Compressing compression/elongation program 138 of the contents manager 111 by the method of predetermined compression of the contents supplied from the sound recording program 113, the encryption program 137 enciphers the compressed contents. Moreover, the use condition conversion program 139 is compressed and generates the data of the use conditions corresponding to the enciphered contents.

[0172] The contents manager 111 is compressed and supplies the enciphered contents to the contents database 114 with the data of use conditions.

[0173] The contents database 114 stores the data of use conditions in the use condition file 162 while it generates the contents file 161 and the use condition file 162 corresponding to the contents which received from the contents manager 111 and stores contents in the contents file 161.

[0174] The contents manager 111 supplies the information on CD received from the sound recording program 113, and the data of use conditions to the display operator guidance program 112, when the data of the use conditions corresponding to contents and contents are stored in the contents database 114.

[0175] The display operator guidance program 112 generates the data for a display stored in the display data file 182 based on the data of the use conditions corresponding to the contents stored in the contents database 114 by processing of sound recording, and the information on CD.

[0176] In the window which the sound recording program 113 displays, when the contents read from

CD are further recorded on the contents database 114, the carbon button 255 which sets up whether the portable device 6-1 thru/or either of 6-3 are made to check out the contents read from CD is arranged automatically.

[0177] For example, when a carbon button 255 is clicked, the sound recording program 113 displays the pull down menu which shows the portable device 6-1 thru/or the list of 6-3. When a user chooses the portable device 6-1 thru/or either of 6-3 from the pull down menu, a personal computer 1 checks out the contents automatically recorded on the selected portable device 6-1 thru/or either of 6-3 from CD. When a user chooses "he not checking out" out from the pull down menu, when contents are recorded from CD, he does not check out a personal computer 1.

[0178] Thus, when the contents read from CD are recorded on the contents database 114 only by activating the carbon button 255 of the window which the sound recording program 113 displays, the contents read from CD to the portable device 6-1 specified beforehand thru/or either of 6-3 can be made to check out a personal computer 1.

[0179] Next, with reference to the flow chart of drawing 7 , the processing in the case of transmitting and copying the contents reproduced from CD with which the drive 22 was equipped to HDD21 by the contents manager 111, the display operator guidance program 112, the sound recording program 113, and CPU11 that performs the contents database 114 is explained. A user operates a keyboard 18 or a mouse 19, and the contents reproduced from CD (not shown) with which the drive 22 was equipped to CPU11 through the interface 17 are transmitted to HDD21. When the command to copy is inputted, the sound recording program 113 In step S11, GUI (Graphical User Interface) shown in drawing 6 in order to choose the contents copied to a display 20 through an interface 17 is displayed.

[0180] The sound recording program 113 reads TOC (Table Of Contents) of CD with which the drive 22 was equipped, acquires the information on the contents contained in the CD, and is made to specifically display it on a display 20. Or the sound recording program 113 reads ISRC (International Standard Recording Code) for every contents contained in CD, acquires the information on the contents, and is made to display it on a display 20. Or when a carbon button 254 is clicked, the sound recording program 113 accesses the WWW server 5-1 or 5-2 through a network 2, acquires the information on the contents of the CD using TOC, and displays the music name corresponding to contents etc. on the field 253 again.

[0181] A user operates a keyboard 18 or a mouse 19 using GUI of a display 20, clicks the check box corresponding to the music name currently displayed on the field 253, and chooses the contents to copy.

[0182] Next, the sound recording program 113 makes the term database (it corresponds to the use condition file 162-1 thru/or 162-N of the contents database 114 shown in drawing 4) stored in the use condition manager 140 at HDD21 check in step S12. The detail of this term database check processing is shown in the flow chart of drawing 8 .

[0183] In step S31, the use condition manager 140 calculates the hash value of the whole term database by having two incomes with CPU32 of an adapter 26, and compares with the calculated value and the hash value saved last time in step S32.

[0184] In addition, when data are not recorded on a term database at all, the use condition manager 140 does not calculate a hash value.

[0185] That is, the term database is formed in HDD21, and as shown in this term database at drawing 9, ISRC and copy time of the contents by which had been recorded in the past as management information which manages the contents (contents) currently recorded on HDD21 correspond, and are memorized. In this example, each ISRC and copy time are memorized about three items of an item 1 thru/or an item 3. In step S38, the hash value of the whole term database based on ISRC and copy time of all contents which are recorded on this term database is calculated by CPU32 of an adapter 26, and is memorized by nonvolatile memory 34 so that it may mention later. A hash value is a value acquired with the application of the Hash Function to data.

[0186] A Hash Function has a property with the difficult inverse transformation which asks for the data of the data which are the function of tropism on the other hand, and were compressed to a basis which carry out a map in the value which compressed the message of the die length of arbitration into the fixed length short. Moreover, it makes it difficult to attach the same value to two messages which the collision of hash values cannot take place easily, namely, are different, for example. A Hash Function is used as a checksum for corroborating that a message is in the middle of a communication link, and was not altered, or is used in a digital signature. As an example of a Hash Function, there are SHA (Secure Hash Algorithm), MD (Message Digest)5, etc.

[0187] In step S31, the use condition manager 140 calculates a hash value, as CPU32 performed. And in step S32, the use condition manager 140 requires read-out of the hash value memorized by nonvolatile memory 34 of CPU32, and compares with it the hash value which received the transfer, and the hash value which is step S31 and he calculated now.

[0188] In step S33 the use condition manager 140 In not judging and being in agreement, whether the hash value now calculated at step S31 and the hash value of the last term database memorized by nonvolatile memory 34 are in agreement It judges with that by which the term database was altered. The use condition manager 140 In step S34, make the sound recording program 113 generate the message "a copy is not made since the term database was altered", make it output to a display 20 through an interface 17, it is made to display, and processing is terminated henceforth. That is, the contents currently recorded on CD are reproduced in this case, and the processing copied to HDD21 is forbidden.

[0189] When the hash value calculated at step S31 and the last hash value are in agreement, it progresses to step S35 and the use condition manager 140 makes ISRC of the contents (selected contents) chosen as contents which were specified as the sound recording program 113 at step S11, and to copy acquire from CD. When ISRC is not recorded on CD, the use condition manager 140 makes the data of TOC of the CD read, and carries out applying a Hash Function to the data etc., for example, obtains the data of suitable die length, such as 58 etc. bits, replaces this with ISRC and uses it for the sound recording program 113.

[0190] In step S36, the use condition manager 140 judges whether ISRC (namely, selected contents) acquired at step S35 is registered into the term database (drawing 9). When ISRC is not registered into a term database, since it will not still be recorded on HDD21, it progresses to step S37 and, as

for the contents, the use condition manager 140 registers ISRC of the contents, and the present time into a term database. In addition, the use condition manager 140 uses the value which RTC35 of an adapter 26 which received the transfer from CPU32 outputs as this current time. And it sets to step S38, and the use condition manager 140 reads the data of the term database at the time, and transmits them to CPU32 of an adapter 26. CPU32 calculates the hash value of the transmitted data, and saves and uses it as nonvolatile memory 34. As mentioned above, the hash value saved by doing in this way is used as a hash value saved last time in step S32.

[0191] Next, in step S39, the use condition manager 140 sets up the non-registered flag showing selected contents not being registered into a term database. In step S13 of drawing 7 mentioned later, this flag is used, when judging whether selected contents are registered into the term database.

[0192] In step S36, when judged with ISRC of selected contents being registered into the term database, it will be said that the selected contents are the contents which may be once registered into HDD21 at least. Then, it progresses to step S40 in this case, and the use condition manager 140 judges whether current time (current time which RTC35 of an adapter 26 outputted) has passed for 48 hours or more from the registration time of those selected contents registered into the term database. Since a lot of [of contents] copy is substantially impossible even if it makes those contents copy again, since 48 hours or more have already passed since that time, although it has recorded on HDD21 at least at once when current time has more nearly already than registration time passed for 48 hours or more, the copy to HDD21 is permitted in this case. Then, it progresses to step S41 and the use condition manager 140 makes the time of a term database change into current time (time which RTC35 outputs) from the past registration time. And return and the use condition manager 140 set a non-registered flag as step S38 to the contents in step S39 while they make CPU32 calculate the hash value of the whole term database and making them save again at nonvolatile memory 34.

[0193] On the other hand, when judged with current time having not passed yet from registration time for 48 hours or more in step S40, the copy to HDD21 of the selected contents is forbidden. Then, in this case, it progresses to step S42 and the use condition manager 140 sets up a registered flag corresponding to those selected contents.

[0194] Generation of a lot of copy of contents required for an unjust sale or distribution etc. becomes impossible substantially, for example, without barring unfairly generation of the copy of contents aiming at the anticipated use which is not inaccurate by processing of step S40, since the new copy of contents is ungenerable if predetermined time amount does not pass. In addition, in step S40, although the criteria of a judgment were considered as progress of 48 hours or more, they should just be the time amount of either not only 48 hours but 12 hours thru/or 168 hours.

[0195] The flag showing whether the contents chosen by term database check processing as mentioned above are registered into HDD21 is set up.

[0196] It judges from the flag which mentioned above whether the selected contents of the copy manager 133 would be registered in a term database in return and step S13 to drawing 7 . When selected contents are registered, it progresses to step S14 and the copy manager 133 makes a

display 20 display a message like the ability "not to copy, since this music has not passed yet for 48 hours or more once it is copied" on the sound recording program 113. Thereby, a user can know the reason which cannot copy the contents to HDD21.

[0197] When judged with selected contents not being registered into a term database, it progresses to step S15, and the sound recording program 113 controls drive 22, and makes contents read from CD with which it is equipped there in step S13. As shown in drawing 1010 at these contents, the water mark code is inserted in the position. In step S16, the sound recording program 113 extracts the water mark code contained in contents, and it judges whether is required or not in step S17 that the water mark code expresses the ban on a copy. When the water mark code expresses the ban on a copy, it progresses to step S18, and the copy manager 133 makes a display 20 display a message like "the copy is forbidden" on the sound recording program 113 through an interface 17, and terminates copy processing.

[0198] On the other hand, when judged with the water mark not expressing the ban on a copy, it progresses to step S19, and the sound recording programs 113 are methods, such as ATRAC (Adaptive Transform Acoustic Coding)³ (trademark), and make contents compress into compression/elongation program 138 by software processing in step S17. The sound recording program 113 is beforehand set as the encryption program 137, and contents are made to encipher in step S20 by the encryption approaches, such as a DES (Data Encryption Standard) method and a FEAL (Fast Encipherment Algorithm) method, using the cryptographic key memorized by memory 13. What was generated in addition to this based on the random number generated with software or the random number generated by CPU32 of an adapter 26 can also be used for a cryptographic key. Thus, it becomes possible CPU32 of not only the personal computer 1 but the adapter 26 as hardware with which it was equipped along with it, and to perform encryption to which decode becomes more difficult because it has two incomes and is made to perform encryption processing.

[0199] Next, the sound recording program 113 transmits the enciphered data to the contents database 114, attaches a file name as one file (as a contents file 161), and is made to save it in step S21 at HDD21. Or the positional information (for example, byte count from a head) of the file name is given, and you may make it save as a part of one file again.

[0200] It may be made to perform this preservation processing, and the above-mentioned compression coding processing and encryption processing separately, and may be made to perform them to coincidence in parallel.

[0201] Furthermore, the sound-recording programs 113 are methods mentioned above, such as a DES method and a FEAL method, make the cryptographic key which enciphered contents encipher, and save in step S22 using the key for preservation memorized by the nonvolatile memory 34 beforehand set to the encryption program 137 in the music database (it corresponds to the use condition file 162-1 thru/or 162-N of the contents database 114 shown in drawing 4) of HDD21.

[0202] In step S23, the sound recording program 113 makes a group the element of the information about the saved file, the enciphered cryptographic key, the information on the contents, and the information on the music name which the user inputted through GUI, and registers it into the music database of HDD21 (it records as the use condition file 162-1 thru/or 162-N). And the sound

recording program 113 makes CPU32 calculate the hash value of the whole music database, and is made to save in step S24 at nonvolatile memory 34.

[0203] Thus, for example, a music database as shown in drawing 11 is registered on HDD21. In this example, accounting conditions, copy conditions (count), the count counter of a copy, and copy conditions (SCMS) are recorded at the time of the file name of an item 1 thru/or an item 3, the enciphered cryptographic key, a music name, the length, playback conditions (initiation time, termination time, count limit), the count counter of playback, and playback.

[0204] For example, by the method which SDMI (Secure Digital Music Initiative) specifies, the count which can check out the contents is set as 3 times corresponding to the contents copied from CD.

[0205] Since it enabled it to reproduce contents again when contents were reproduced by HDD21 from CD and a fixed period passed, several duplicates made into the range of user's individual's use are attained. On the other hand, if it is going to reproduce in large quantities across the range of individual use, immense time amount will be needed and it will become impossible actually. Moreover, a personal computer 1, for example, when the contents currently recorded on HDD21 are eliminated, the eliminated contents can be again reproduced after progress of a fixed period, and it can record on HDD21.

[0206] Moreover, for example, the contents of the term database currently recorded on HDD21 through the network 2 are also sharable.

[0207] Although the case where the time reproduced above corresponding to ISRC was memorized was explained as an example, if it is the information which identifies contents and CD, other things (for example, a music name, album names, those combination, etc.) can also be used.

[0208] Next, with reference to the flow chart of drawing 12 thru/or drawing 14, the processing by CPU52 which performs CPU11 and the main program which perform the display operator guidance program 112 and the contents manager 111 which moves contents to the flash memory 61 (for example, memory stick (trademark)) of the portable device 6 from HDD21, and processing of check-out are explained.

[0209] Processing of migration of introduction and contents is explained. In step S51, the migration manager 134 makes the use condition manager 140 calculate the hash value of the whole music database, it is step S52, and CPU32 is made to calculate it last time, and it compares with the hash value saved at nonvolatile memory 34. When both are not in agreement, after the migration manager 134 progresses to step S53 and makes a display 20 display a message like "there is a possibility that the music database might be altered" on the display operator guidance program 112, it terminates processing. The processing in this case is the same processing as processing of step S31 of drawing 8 thru/or step S34. In this case, migration of contents to the portable device 6 from HDD21 will be performed.

[0210] Next, the migration manager 134 reads the information on the contents registered there from the music database (contained in the contents database 114) currently formed in HDD21, and a display 20 is made to display it on the display operator guidance program 112 as GUI for selection in step S54. A user clicks and chooses from HDD21 a music name, a carbon button 216, etc. which

are displayed on the field 212 of drawing 5 in the contents which make it move to the portable device 6 based on GUI for this selection. Next, in step S55, the migration manager 134 investigates accounting conditions etc. at the time of the playback conditions of the selected contents chosen at step S54, copy conditions, and playback. The detail of this processing is later mentioned with reference to the flow chart of drawing 15.

[0211] Next, in step S56, mutual recognition processing is performed between the authentication program 141 of a personal computer 1, and CPU53 of the portable device 6, and the key for a communication link is shared.

[0212] For example, the master key KM shall be beforehand memorized by the flash memory 61 (or EEPROM68) of the portable device 6, and the individual keys KP and ID shall be beforehand memorized by RAM13 (or predetermined file of HDD21) of a personal computer 1. CPU53 receives supply of ID beforehand memorized by RAM13 from the authentication program 141, applies a Hash Function to the master key KM which the ID and themselves have, and generates the same key as the individual key of the personal computer 1 memorized by RAM13. A common individual key will be shared between doing in this way by both a personal computer 1 and the portable device 6. A still more temporary key for a communication link is generable using this individual key.

[0213] Or while making RAM13 of a personal computer 1 memorize ID and the master key KMP beforehand, the flash memory 61 of the portable device 6 is also made to memorize ID and the master key KMM of the portable device 6 again. And by transmitting each ID and master key to each other on another side, another side applies a Hash Function to ID and the master key which have been transmitted from one side, and generates the individual key of another side. And a temporary key for a communication link is further generated from the individual key.

[0214] In addition, as the approach of authentication, it is IOS (International Organization for Standardization), for example. 9798-2 can be used.

[0215] When mutual recognition is not performed correctly, processing is ended, but when carried out correctly, further, in step S57, the migration manager 134 makes the file name of the contents chosen as the contents database 114 read from a music database, and reads the contents (for example, enciphered by processing of step S20 of drawing 7) of the file name from HDD21. In step S58, the migration manager 134 performs processing which changes into the thing of the portable device 6 the compression coding method (processing of step S19) of the contents which are digital data read at step S57, a cipher system (processing of step S20), formats (for example, method of a header etc.), etc. The detail of this transform processing is later mentioned with reference to the flow chart of drawing 17.

[0216] The migration manager 134 makes the contents changed into the driver 143 for PD at step S58 transmit to the portable device 6 through the USB port 23 in step S59. CPU53 of the portable device 6 makes a flash memory 61 memorize those contents as it is in step S60, when these transmitted contents are received through the USB connector 56.

[0217] In step S61, the migration manager 134 is further changed into the format that the portable device 6 has managed the playback conditions (initiation time, termination time, count limit, etc.) of the selected contents registered into the music database by the use condition conversion program

139. In step S62, the migration manager 134 transforms the SCMS information in the copy condition further registered into the music database of the contents chosen as the use condition conversion program 139 to the format which the portable device 6 manages. And the migration manager 134 makes the playback conditions changed into the driver 143 for PD at step S61, and the SCMS information changed at step S62 transmit to the portable device 6 in step S63. CPU53 of the portable device 6 saves the playback conditions and SCMS information that the transfer was received at a flash memory 61.

[0218] The migration manager 134 is made to transmit to the portable device 6, and is made to save in step S64 at a flash memory 61 with the playback conditions registered into the music database of the contents chosen as the driver 143 for PD again, and the format that CPU11 is treating accounting conditions, copy conditions, etc. in the music database at the time of playback.

[0219] The migration manager 134 makes the cryptographic key as which the contents chosen as the contents database 114 are enciphered read from a music database, it makes the decode program 142 decode the cryptographic key with the key for preservation saved at RAM13, and it is made to encipher it with the key for a communication link to the encryption program 137 in step S66 in step S65. And the migration manager 134 makes the driver 143 for PD transmit the cryptographic key enciphered with the key for a communication link to the portable device 6.

[0220] CPU53 of the portable device 6 is step S67, the cryptographic key transmitted from the personal computer 1 is decoded using the key for a communication link shared between mutual recognition processing, it enciphers using its own key for preservation, and is related with the already saved data, and is saved at a flash memory 61.

[0221] CPU53 will notify having saved the cryptographic key to the personal computer 1 in step S68, if preservation of a cryptographic key is completed. It makes the group (namely, use condition file 162) of the element of those contents delete from a music database in step S69, if the migration manager 134 of a personal computer 1 receives this notice from the portable device 6 while making the contents database 114 delete the contents file 161 corresponding to those contents. That is, not a copy but migration (MUBU) will be performed by this. And the migration manager 134 transmits the data of a music database to CPU32 of an adapter 26, makes it calculate the whole hash value, and is made to save in step S70 at nonvolatile memory 34. This hash value will be used as a hash value saved last time in step S52 mentioned above.

[0222] Next, the processing which checks out contents from a personal computer 1 to the portable device 6 is explained. The processing which checks out contents from the personal computer 1 to the portable device 6 is the same processing as the case where contents are moved to the portable device 6 from the personal computer 1 of drawing 12 thru/or drawing 14 . Namely, processing of check-out is performed by check-in/check-out manager 132 in a personal computer 1, and is set to step S69 of drawing 14 . Replace with the processing which deletes contents and are recorded on the music database. Since it becomes the processing in migration with the same processing fundamentally except for performing processing which updates the count (or count which can be checked out) which the checked-out contents checked out, explanation of the detail of the processing is omitted.

[0223] Next, the check processing of the playback conditions of the selected contents in step S55 of

drawing 12 etc. by CPU11 which performs the contents manager 111 is explained with reference to the flow chart of drawing 15 . The migration manager 134 makes various kinds of conditions read from a music database to the contents database 114 in step S81. The migration manager 134 judges whether the count of a copy has already passed over the count of a copy limit among the various conditions read at step S81 in step S82. Since a copy cannot be permitted any more when the count of a copy has already passed over the count of a copy limit, it progresses to step S83, and the migration manager 134 makes the display operator guidance program 112 display a message like "the count of a copy has already become the count of a copy limit" on a display 20, and makes it end processing. In step S82, when it judges that the count of a copy has not passed over the count of a copy limit, it progresses to step S84 and the judgment of whether current time has passed over playback termination time is performed. As current time, what was outputted from RTC35 of an adapter 26 is used. What that by which the user corrected the current time of a personal computer 1 to the past value intentionally is used by this is prevented. The migration manager 134 supplies the playback conditions which step S84 is itself judged in response to offer from CPU32, or are step S81, and read this current time from the music database to CPU32 of an adapter 26, and makes CPU32 perform judgment processing of step S84.

[0224] It progresses to step S85, and the migration manager 134 makes the information on the selected contents eliminate from a music database, when current time has passed over playback termination time while making the contents chosen as the contents database 114 eliminate from HDD21. The migration manager 134 makes CPU32 calculate the hash value of a music database, and makes it save in step S86 at nonvolatile memory 34. Henceforth, processing is ended. Therefore, migration of contents is not performed in this case.

[0225] In step S84, when judged with the time of present in Japan having not passed over playback termination time, it progresses to step S87 and the migration manager 134 judges whether accounting conditions (for example, tariff per playback) are registered into the music database at the time of playback of the selected contents. When accounting conditions are registered at the time of playback, in step S88, the migration manager 134 makes the driver 143 for PD communicate with the portable device 6, and judges whether an accounting function exists in the portable device 6. Since selected contents cannot be transmitted to the portable device 6 when an accounting function does not exist in the portable device 6, the migration manager 134 makes the display operator guidance program 112 display a message like "the destination does not have the accounting function" on a display 20, and makes it end migration processing of contents in step S89.

[0226] When judged with accounting conditions not being registered in step S87 at the time of playback, or when it is judged with an accounting function existing in the portable device 6 in step S88, it progresses to step S90 and the migration manager 134 judges whether the playback conditions of others, such as a count of a playback limit, are registered, concerning selected contents. When other playback conditions are registered, it progresses to step S91 and the migration manager 134 judges whether the function to keep the playback condition to the portable device 6 exists. When the portable device 6 does not have the function to keep the playback condition, it progresses to step S92, and the migration manager 134 makes the display operator guidance

program 112 display a message like "not having the function in which the equipment of the destination keeps playback conditions" on a display 20, and makes it end processing.

[0227] In step S90, when judged with playback conditions not being registered, or when it judges that the portable device 6 has the function to keep playback conditions in step S91, check processing of playback conditions etc. is ended and it returns to step S56 of drawing 12.

[0228] Drawing 16 expresses the example of the playback conditions which the portable device 6 has managed (protecting is possible). The playback information shown in drawing 16 is memorized by EEPROM68. In this example, although playback initiation time and playback termination time are registered about each contents of an item 1 thru/or an item 3, the count of playback is registered only about the item 2, and is not registered about an item 1 and an item 3. Therefore, although the playback conditions of the count of playback can be protected when it considers as the contents as which the contents of an item 2 were chosen, when it considers as the contents as which the contents of an item 1 or an item 3 were chosen, the conditions of the count of playback can be kept.

[0229] Next, with reference to the flow chart of drawing 17, the detail of the format conversion processing in step S58 of drawing 12 by CPU11 which performs the contents manager 111 is explained. In step S101, the migration manager 134 investigates a format (for example, methods, such as a header including playback conditions, a service condition, copy conditions, etc.) of the selected contents currently recorded on the contents database 114. In step S102, the migration manager 134 investigates the conditions which can be set as a phase hand's device (in the case of now portable device 6). That is, the migration manager 134 asks the conditions which can be set as CPU53 of the portable device 6, and obtains the reply. In step S103, the migration manager 134 determines the conditions which can be set as a phase hand's device among the conditions of the format registered into the music database based on the conditions investigated at step S102.

[0230] In step S104, when it judges whether the conditions which can be set up exist and the conditions which can be set up do not exist, the migration manager 134 progresses to step S105, and forbids the processing which moves contents to the portable device 6. That is, since the portable device 6 cannot keep the conditions registered into the music database in this case, it is prohibited to such a portable device 6 from moving contents.

[0231] When judged with the conditions which can be set up existing in step S104, it progresses to step S106 and the use condition conversion program 139 is made to change the migration manager 134 into the conditions (for example, conditions stored in a header in case it transmits to the portable device 6) of a functional format of the condition of a phase hand. And in step S107, the migration manager 134 sets the changed conditions as a phase hand's device. Consequently, the portable device 6 becomes possible [reproducing contents] according to the set-up conditions (keeping the condition).

[0232] Next, with reference to the flow chart of drawing 18 thru/or drawing 20, the processing in the case of copying contents to the portable device 6 from HDD21 by CPU53 which performs CPU11 and the main program which perform the contents manager 111 is explained. Processings of step S111 of this drawing 18 thru/or drawing 20 thru/or step S127 are processing of step S51 in the case of the copy manager 133 performing and moving contents to the portable device 6 from HDD21 of

drawing 12 thru/or drawing 14 thru/or step S67, and the same processing. That is, also in this case, after the alteration of a music database is checked, check processing with the playback conditions of selected contents is performed. Furthermore, contents are transmitted and saved from HDD21 of a personal computer 1 at the flash memory 61 of the portable device 6 after the mutual recognition processing between the portable device 6 and a personal computer 1. Then, in step S128, as for the copy manager 133, only 1 increments the count counter of a copy of a music database. And the copy manager 133 makes CPU32 calculate the hash value of the whole music database, and makes the value save in step S129 at nonvolatile memory 34.

[0233] Next, with reference to the flow chart of drawing 21 , the processing by CPU53 which performs CPU11 and the main program which perform the contents manager 111 which moves contents to HDD21 from the portable device 6, and processing of check-in are explained.

[0234] Processing of migration of introduction and contents is explained. In step S161, the migration manager 134 requires read-out of the information on the contents memorized by the flash memory 61 to CPU53 of the portable device 6. CPU53 transmits the information on the contents memorized by the flash memory 61 to a personal computer 1 corresponding to this demand. The migration manager 134 displays GUI for choosing as a display 20 the contents memorized by the flash memory 61 based on this information. A user operates a keyboard 18 or a mouse 19, and specifies the contents which make it move to HDD21 (contents database 114) from the portable device 6 based on the GUI.

[0235] The migration manager 134 makes the authentication program 141 perform mutual recognition processing between CPUs53, and makes it share the key for a communication link in step S162. This processing is the same processing as the case in step S56 of drawing 12 .

[0236] Next, in step S163, CPU53 reads the selected contents which are memorized by the flash memory 61 and which are enciphered, and transmits them to a personal computer 1. In step S164, the migration manager 134 attaches a file name as one file, and saves the contents transmitted from the portable device 6 in the contents database 114 (HDD21). This preservation can be performed as a part of one file by giving the positional information (for example, byte count from a head) of a file name.

[0237] In step S165, CPU53 reads the cryptographic key as which the selected contents memorized by the flash memory 61 are enciphered, decodes it with its own key for preservation, and after enciphering with the key for a communication link further, it transmits it to a personal computer 1. This cryptographic key is saved by processing of step S67 of drawing 14 at the flash memory 61.

[0238] When a transfer of a cryptographic key is received from the portable device 6, the migration manager 134 makes the decode program 142 decode it with the key for a communication link, and it is made to encipher it with its own key for preservation to the encryption program 137 in step S166. The migration manager 134 makes the music name which the file name of the contents saved at step S164, the information on the contents, and a user inputted into the contents database 114 through GUI, the cryptographic key enciphered at step S166 register into the music database of HDD21 at step S167. And the migration manager 134 makes CPU32 calculate the hash value of the whole music database to the use condition manager 140, and is made to save in step S168 at

nonvolatile memory 34 at it.

[0239] In step S169, the migration manager 134 notifies that the cryptographic key was saved to the portable device 6, and requires deletion of the contents. CPU53 deletes the contents memorized by the flash memory 61 from a personal computer 1 in step S170, when deletion of the contents has been required.

[0240] Next, the processing which checks in at contents is explained to a personal computer 1 from the portable device 6. The processing which checks in at contents from the portable device 6 at a personal computer 1 is the same processing as the case where contents are moved to a personal computer 1 from the portable device 6 of drawing 21. That is, processing of check-in is performed by check-in/check-out manager 132 in a personal computer 1, and step S162 of drawing 21 thru/or processing of S166 are omitted. Moreover, since a personal computer 1 serves as processing in migration with the same processing fundamentally except for checking deletion of a contents file after processing of step S170 by performing processing which is recorded on the music database and which updates the count which can check out the contents at which he checked in in step S167 of drawing 21, explanation of the detail of the processing is omitted.

[0241] In addition, when the flash memory 61 of the portable device 6 is removable as a memory card, a personal computer 1 performs processing of the mutual recognition of step S162 of drawing 21 in processing of check-in.

[0242] moreover -- if the contents which the contents by which the predetermined personal computer was checked out can check in now only at this personal computer as mentioned above, and were chosen as pretreatment of check-in processing judge whether PC at which he checks in was checked out and judged not to be that by which this PC was checked out -- if -- the step processed so that he may not check in exists. For example, the case where he tries to check in at the contents which x of the field 213 of drawing 5 attached hits it.

[0243] Next, the processing in the case of copying contents to HDD21 from the portable device 6 by CPU53 which performs CPU11 and the main program which perform the contents manager 111 is explained with reference to the flow chart of drawing 22. Processings of step S181 thru/or step S188 shown in this drawing 22 are processing of step S161 in the processing in the case of moving contents to HDD21 from the portable device 6 of drawing 21 thru/or step S168, and the same processing. That is, since it becomes the processing in migration with the same processing fundamentally except for the point that the copy manager 133 performs and processing of steps S169 and S170 of drawing 21 is omitted in copy processing, the explanation is omitted.

[0244] Next, with reference to the flow chart of drawing 23, the processing which copies the contents which received the transfer from the EMD server 4 by CPU11 which performs the EMD server 4 and the contents manager 111 to HDD21 is explained. When the carbon button 202 shown in drawing 5 is clicked and it is ordered in access to the EMD server 4 from a user, the program 144 for purchase controls the communications department 25, and is made to access the EMD server 4 through a network 2 in step S201. The EMD server 4 transmits information, such as a tune number number of the contents which he holds, a music name, and each information, to a personal computer 1 through a network 2 corresponding to this access. The program 144 for purchase makes

a display 20 display it on the display operator guidance program 112 through an interface 17, when this information is acquired through the communications department 25. A user specifies the contents which wish to copy in step S202 using GUI displayed on the display 20. This assignment information is transmitted to the EMD server 4 through a network 2. In step S203, the program 144 for purchase performs mutual recognition processing through a network 2 between the EMD servers 4, and shares the key for a communication link.

[0245] The mutual recognition processing performed between a personal computer 1 and the EMD server 4 is ISO. It can carry out using the public key and private key which are specified by 9798-3. In this case, the personal computer 1 has beforehand its own private key and the public key of the EMD server 4, the EMD server 4 has its own private key, and mutual recognition processing is performed. It transmits from the EMD server 4, or the certificate (certificate) beforehand distributed to the personal computer 1 is transmitted to the EMD server 4 from a personal computer 1, the EMD server 4 checks the certificate, and you may make it the public key of a personal computer 1 obtain a public key. Furthermore, in step S204, the program 144 for purchase performs processing about accounting in between the EMD servers 4. The detail of processing of this accounting is later mentioned with reference to the flow chart of drawing 24.

[0246] Next, in step S205, the EMD server 4 transmits the contents which were specified at step S202 and which are enciphered to a personal computer 1 through a network 2 to a personal computer 1. At this time, time information is also transmitted suitably. The program 144 for purchase attaches a file name to the contents which received the transfer, and is made to save it as one contents file 161 in the contents database 114 in step S206 at HDD21. In step S207, it enciphers further using the key for a communication link which shared the cryptographic key of the contents between step S203 with the personal computer 1, and the EMD server 4 is transmitted to a personal computer 1.

[0247] The program 144 for purchase makes the cryptographic key which are independent, or the decode program 142 was made to decode the cryptographic key which received the transfer from the EMD server 4 using the key for a communication link in collaboration with CPU32 of an adapter 26, decoded to the encryption program 137, and was obtained encipher with its own key for preservation in step S208. The program 144 for purchase makes a group the music name which the file name of the contents, the information on contents, and a user inputted into the contents database 114, and the enciphered cryptographic key, and is made to register it into the music database of HDD21 in step S209. Furthermore, the program 144 for purchase makes CPU32 calculate the hash value of the whole music database, and is made to save in step S210 at nonvolatile memory 34.

[0248] In addition, in step S205, the EMD server 4 transmits time-of-day data to a personal computer 1 with contents. This time-of-day data is transmitted to an adapter 26 from a personal computer 1. CPU32 of an adapter 26 makes the time of day of RTC35 correct in step S211, when the time-of-day data transmitted from the personal computer 1 are received. Thus, since the time information of RTC35 of an adapter 26 was corrected based on the time information acquired from the equipment of the exterior recognized to be right equipment as a result of mutual recognition, it

becomes possible about an adapter 26 to always hold right time information.

[0249] Next, with reference to the flow chart of drawing 24, the detail of the processing about accounting in step S204 of drawing 23 by CPU11 which performs the EMD server 4 and the contents manager 111 is explained. In step S221, the program 144 for purchase reads the price information of the selected contents specified at step S202 out of the price information transmitted from the EMD server 4 at step S201, and writes this in the accounting log on HDD21. Drawing 25 expresses the example of such an accounting log. In this example, the user has copied the item 1 thru/or the item 3 from the EMD server 4, the field of an item 1 and an item 2 is made into 50 yen, and the tariff of an item 3 is made into 60 yen. The hash value of the accounting log at the time is also calculated by CPU32, and is registered into nonvolatile memory 34.

[0250] Next, in step S222, the program 144 for purchase reads the accounting log written in at step S221 from HDD21, and transmits this to the EMD server 4 through a network 2. The EMD server 4 performs accounting computation based on the accounting log which received the transfer from the personal computer 1 in step S223. That is, the EMD server 4 carries out renewal of an addition of the accounting log transmitted to the database to build in by the user of a personal computer 1. And in step S224, in judging whether the EMD server 4 approves immediately about the accounting log and approving immediately, it progresses to step S225 and the EMD server 4 transmits a trade name required for sanction, the amount of money, etc. to a sanction server (not shown). And in step S226, a sanction server performs sanction processing to the user of a personal computer 1. In step S224, when judged with sanction not having a limping gait crack immediately, processing of steps S225 and S226 is skipped. Namely, this processing is periodically performed once etc. after that per month.

[0251] Next, with reference to the flow chart of drawing 26 and drawing 27, the processing in the case of copying the contents reproduced from the CD player which is not illustrated to HDD21 in which it was inputted from IEC60958 terminal 24a of the voice-input/output interface 24 by CPU11 which performs the contents manager 111 is explained. In step S241, a user connects IEC60958 output terminal of a CD player to IEC60958 terminal 24a of the voice-input/output interface 24 of a personal computer 1. In step S242, a user operates a keyboard 18 or a mouse 19, and inputs the music name (or number corresponding to contents) of the contents copied from a CD player. And a user operates the carbon button of a CD player and makes playback of a CD player start in step S243. When the line which sends and receives a control signal between a CD player and a personal computer 1 is connected, it is possible to also make a CD player start playback of CD in inputting a playback initiation command through the keyboard 18 or mouse 19 of a personal computer 1.

[0252] In a CD player, initiation of playback of CD transmits the contents outputted from the CD player to a personal computer 1 through IEC60958 terminal 24a in step S244. In step S245, the copy manager 133 reads SCMS (Serial Copy Management System) data in the data inputted through IEC60958 terminal 24a. It restricts to this SCMS data the ban on a copy, and one copy, and copy information, such as possibility of and a copy free-lancer, is included in it. In step S246, when it judges whether SCMS data express the ban on a copy and the ban on a copy is expressed, CPU11 progresses to step S247, and the copy manager 133 displays on a display 20 the message that "copy

is forbidden to the display operator guidance program 112", and it ends copy processing there. That is, the copy to HDD21 is forbidden in this case.

[0253] In step S246, when it judges with the SCMS information read at step S245 not expressing the ban on a copy, the copy manager 133 progresses to step S248, reads a water mark code, and judges whether the water mark expresses the ban on a copy in step S249. When the water mark code expresses the ban on a copy, like the case where it progressed and mentions above to step S247, a predetermined message is displayed and copy processing is ended.

[0254] In step S249, when judged with the water mark not expressing the ban on a copy, it progresses to step S250 and term database check processing is performed. If selected contents are already registered as a result of the term database check, processing will be ended by processing of steps S251 and S252. This processing is the same processing as processing of steps S13 and S14 of drawing 7.

[0255] If selected contents are the contents which are not registered into HDD21 yet, the registration processing will be performed by step S253 thru/or S258. Since processings of this step S253 thru/or step S258 are processing of step S19 of drawing 7 thru/or step S24, and the same processing except for the point that the SCMS information supplied from IEC60958 terminal 24a is also registered into a music database in step S257, that explanation is omitted.

[0256] Next, with reference to the flow chart of drawing 28 and drawing 29, the processing in the case of outputting contents to IEC60958 terminal 24a from HDD21 (playback) by CPU11 which performs the contents manager 111 is explained. In step S271 thru/or step S273, like the case in step S111 of drawing 18 thru/or S113, the hash value of the whole music database is calculated, it is judged whether it is in agreement with the hash value saved last time, and check processing of an alteration of a music database is performed. It progresses to step S274, and when judged with the alteration of a music database not being performed, through the contents manager 111, the display operator guidance program 112 makes the music database of HDD21 access the contents database 114, it makes the information on the music registered there read, and is displayed on a display 20. A user looks at the display, operates a keyboard 18 or a mouse 19 suitably, and chooses the contents which carry out a playback output. In step S275, the display operator guidance program 112 performs check processing of the playback conditions of selected contents etc. Details of check processing, such as this playback condition, are later mentioned with reference to the flow chart of drawing 30.

[0257] Next, the display operator guidance program 112 makes the cryptographic key of the contents chosen as the contents database 114 in step S274 read from a music database through the contents manager 111, and the decode program 142 is made to decode it with the key for preservation in step S276. In step S277, the display operator guidance program 112 makes the SCMS information on the contents chosen as the contents database 114 read from a music database through the contents manager 111, and determines the SCMS information outputted from IEC60958 terminal 24a according to the regulation of a SCMS system. For example, when the count of playback has a limit, the increment only of 1 is carried out and let the count of playback be new SCMS information. The display operator guidance program 112 makes ISRC of the contents chosen

as the contents database 114 read from a music database through the contents manager 111 further in step S278.

[0258] Next, the display operator guidance program 112 makes the contents file name chosen as the contents database 114 from the music database read through the contents manager 111, and makes the contents read from HDD21 based on the file name in step S279. The display operator guidance program 112 decodes the contents enciphered using the cryptographic key which made read the cryptographic key corresponding to the contents from a music database to the contents database 114, and the decode program 142 was made to decode with the key for preservation through the contents manager 111 further, and was decoded. Compression/elongation program 138 decodes the compression sign of the contents further (elongation). The display operator guidance program 112 is made to output from IEC60958 terminal 24a in step S280 according to a convention of IEC60958 with the SCMS information which determined the contents which are step S279 and are decoded digital data as the driver 117 at step S277, and the ISRC information read to the list at step S278. The display operator guidance program 112 operates programs, such as a real player (trademark) which is not illustrated, for example, makes the contents which are digital data analog-ize, and is made to output from the analog output terminal of the voice input/output interface 24 further again.

[0259] In step S281, as for the display operator guidance program 112, only 1 carries out the increment of the value of the count counter of playback in a music database to the contents database 114 through the contents manager 111. And in step S282, it judges whether accounting conditions are added to selected contents at the time of playback. When accounting conditions are added at the time of playback, the display operator guidance program 112 makes the tariff corresponding to the contents database 114 write in an accounting log, and the display operator guidance program 112 makes CPU32 calculate the hash value of the whole music database to the use condition manager 140, and it makes it to progress to step S283 and memorize it to nonvolatile memory 34 in step S284 through the contents manager 111. In step S282, when judged with accounting conditions not being added to selected contents at the time of playback, processing of step S283 and step S284 is skipped.

[0260] Next, with reference to the flow chart of drawing 30, details of check processing, such as playback conditions of step S275 of drawing 28 by CPU11 which performs the contents manager 111, are explained. The display operator guidance program 112 makes the various conditions of a music database read to the contents database 114 through the contents manager 111 in step S301. In step S302, the count of playback among the conditions which the use condition manager 140 read judges whether it has passed over the count of a limit, and while making the contents chosen as the contents database 114 delete from HDD21 through the contents manager 111, the information on the contents chosen from the music database is made to progress to step S303, and to delete, when having passed. The display operator guidance program 112 makes CPU32 calculate the new hash value of a music database to the use condition manager 140, and makes the hash value save further in step S304 at nonvolatile memory 34 at it. In this case, a playback output is forbidden.

[0261] In step S302, when it judges that the count of playback has not passed over the count of a limit, it progresses to step S305 and the use condition manager 1402 judges whether playback

termination time has passed over current time. When playback termination time has passed over current time, while making selected contents delete from HDD21 in step S303 like the case where it mentions above, it is made to delete also from a music database. And the hash value of a new music database is calculated and saved in step S304. Also in this case, a playback output is forbidden.

[0262] In step S305, when it judges that playback termination time has not passed over current time, it progresses to step S306 and CPU32 judges whether accounting conditions are added to the selected contents at the time of playback. When accounting conditions are added at the time of playback, it progresses to step S307 and the display operator guidance program 112 displays on a display 20 the message and tariff of a purport to which accounting conditions are added at the time of playback. In step S306, when judged with accounting conditions not being added at the time of playback, processing of step S307 is skipped.

[0263] Next, with reference to the flow chart of drawing 31 and drawing 32, the processing in the case of outputting contents by portable device 6 course from HDD21 (playback) by CPU53 which performs CPU11 and the main program which perform the contents manager 111 is explained. In step S321 thru/or step S325, check processing of the alteration check of a music database, assignment of selected contents, the playback conditions of the contents chosen as the list, etc. is performed. Since the processing is the same processing as processing of step S271 of drawing 28 thru/or step S275, the explanation is omitted.

[0264] In step S326, mutual recognition processing is performed between the portable device 6 and a personal computer 1, and the key for a communication link is shared between mutual. In step S327, the display operator guidance program 112 is ordered to reproduce the contents which will be sent from now on and which are enciphered to the portable device 6. The display operator guidance program 112 makes the file name of the selected contents which are step S324 and were specified as the contents database 114 through the contents manager 111 read from a music database, and makes the contents of the file name read from HDD21 in step S328. The display operator guidance program 112 performs processing which changes the compression coding method of contents, a cipher system, a format, etc. into the contents manager 111 at the thing of the method of the portable device 6 in step S329. And in step S330, the display operator guidance program 112 makes the contents changed into the encryption program 137 in step S329 encipher with the key for a communication link, and is transmitted to the portable device 6.

[0265] In step S327, corresponding to the instruction transmitted from the personal computer 1, CPU53 of the portable device 6 decodes each data which received the transfer with the key for a communication link, and carries out a playback output in step S331. In step S332, as for the display operator guidance program 112, only 1 carries out the increment of the count count of playback of a music database to the contents database 114 through the contents manager 111. Furthermore, CPU32 is made to newly calculate [in / make an accounting log write / in / when it judges whether accounting conditions are added to the contents as which the display operator guidance program 112 was chosen in step S333 at the time of playback and is added / step S334 / the tariff in the contents database 114 through the contents manager 111, and / step S335] the hash value of the whole music database, and it is made to save. When accounting conditions are not added to selected

contents at the time of playback, processing of step S334 and step S335 is skipped.

[0266] In this invention, in order to prevent that contents are reproduced unjustly, various kinds of creativity is put. For example, let the program which operates CPU11 be the so-called tamper REJISUTANTO software with which the execution sequence changes each time.

[0267] Furthermore, as mentioned above, a part of function of CPU11 is shared with the adapter 26 as hardware, and it is made as [perform / both have two incomes and / various kinds of processings]. It is possible for this to raise safety more.

[0268] For example, as mentioned above, the hash value of a music database is saved at the nonvolatile memory 34 of an adapter 26 rather than is saved at the music database itself. That is, in comparison processing with the hash value saved last time [, such as steps S32 and S33 of drawing 8 ,], the hash value of the past made applicable to a comparison shall memorize at nonvolatile memory 34. By this for example, before making it copy or move to other record media All the contents of record containing the contents saved at HDD21 are backed up. After copying or moving the contents saved there to other record media from HDD21, the contents contained in the contents of record which backed up to HDD21 by making it restore again Use conditions are disregarded, there are no limits substantially, and it is prevented that copy or migration can be performed.

[0269] For example, as shown in drawing 33 , when Contents A and B are saved at HDD21, the hash value corresponding to the information on Contents A and Contents B is saved at nonvolatile memory 34. Suppose that some or all containing the contents A and B of HDD21 of record data was backed up to other record media 271 in this condition. Then, since the contents currently recorded on HDD21 at the time turn into Contents B when Contents A are moved to other record media 272 among the contents A saved at HDD21, and Contents B, the hash value of nonvolatile memory 34 is also changed into the hash value corresponding to Contents B.

[0270] Therefore, even if it restores some or all containing the contents A and B of HDD21 which backed up to the record medium 271 of record data to HDD21 and makes Contents A and Contents B save again after that at HDD21, the hash value calculated from the information on Contents B is memorized by nonvolatile memory 34, and the hash value calculated from the information on Contents A and Contents B is not memorized. The hash value based on Contents A and Contents B which are memorized by HDD21 at the time will not be in agreement with the hash value of the past memorized by nonvolatile memory 34 by this, and it is detected that the music database was altered. Consequently, use of Contents A and Contents B which are saved at HDD21 will be restricted henceforth.

[0271] Furthermore, as mentioned above, the adapter 26 contains RTC35 and the value of this RTC35 corrects that time information based on the time-of-day data transmitted from other equipments (for example, EMD server 4) with which the right authentication result was obtained. And as current time, a personal computer 1 does not manage and what RTC35 outputs is used. Therefore, it becomes impossible that a user corrects the current time of a personal computer 1 at the past time of day intentionally, and escapes the judgment of the playback termination time as playback conditions.

[0272] Moreover, an adapter 26 is constituting so that the program enciphered and transmitted may

be decoded and performed according to the program memorized beforehand to ROM36, and safety is raised more. Next, this point is explained with reference to the flow chart of drawing 34.

[0273] That is, in step S351, it enciphers using the cryptographic key memorized beforehand to RAM13 and a personal computer 1 transmits the program which an adapter 26 should be made to perform to an adapter 26 to perform predetermined processing to an adapter 26. The program for decoding and performing the program enciphered transmitted from the personal computer 1 is beforehand memorized by ROM36 of an adapter 26. CPU32 decodes the program which has been transmitted from the personal computer 1 and which is enciphered in step S352 according to the program memorized by this ROM36. And in step S313, CPU32 develops the decoded program to RAM33, and performs the program in step S354.

[0274] For example, as mentioned above, when making an adapter 26 calculate the hash value of the music database of HDD21, CPU11 of a personal computer 1 enciphers the data of a music database by the cryptographic key, and transmits them to CPU32 of an adapter 26. CPU32 is adapted in a Hash Function to the data of the transmitted music database, and calculates a hash value. And nonvolatile memory 34 is made to memorize the calculated hash value. Or as compared with the hash value of the past when CPU32 is beforehand memorized in the hash value, a comparison result is transmitted to CPU11 of a personal computer 1.

[0275] Drawing 35 expresses the more concrete configuration inside an adapter 26. An adapter 26 is formed as a semiconductor IC. The adapter 26 has the logical circuit 302 in the RAM controller 301 and list which control the writing to RAM33, and read-out in addition to interface [which was shown in drawing 2] 31, CPU32 and RAM33, nonvolatile memory 34, RTC35, and ROM36. A logical circuit 302 is used for processing of a case so that the direct output of the decoded data may be carried out from an adapter 26, after decoding the contents enciphered for example.

[0276] A logical circuit 302 is included in these interfaces 31 thru/or ROM36, the RAM controller 301, and a list in one in a semiconductor IC, and it consists of the exteriors so that it cannot decompose.

[0277] A quartz resonator 311 is used when generating the clock with which an adapter 26 performs various kinds of processings upwards, and serves as criteria. An oscillator circuit 312 is an oscillator circuit for operating RTC35. The dc-battery 313 supplies the power for backup to an oscillator circuit 312, nonvolatile memory 34, and RTC35. The power from the current supply circuit 321 of a personal computer 1 is supplied to the circuit of others of an adapter 26.

[0278] Although it is also possible to constitute from a ROM in which write-in elimination is possible, when it constitutes from RAM backed up by the backup power supply from a dc-battery 313, the protection aluminum layer 351 is formed on nonvolatile memory 34, and as shown in drawing 36, nonvolatile memory 34 can form further the power-source pattern 352 which supplies the power from a dc-battery 313 to nonvolatile memory 34 so that it may become the same flat-surface top as the protection aluminum layer 351. That nonvolatile memory 34 should be altered, for example if it does in this way, when it is going to delete the protection aluminum layer 351, the power-source pattern 352 on the same flat surface will also be deleted, supply of the power to nonvolatile memory 34 will be cut off, and the data memorized inside will be eliminated. Thus,

with constituting, tamper resist nature can be raised more.

[0279] Furthermore, as shown in drawing 37, the wiring 401-1 for the writing of data to nonvolatile memory 34 or read-out thru/or 401-3 are corresponding locations, and it is formed so that it may overlap in the vertical (depth) direction. In order to read data from the wiring 401-3 of thereby more a lower layer, it becomes impossible to have to remove the upper wiring 401-1,401-2, and to read data in two or more wiring 401-1,401-2,401-3 to coincidence.

[0280] Nonvolatile memory 34 can form wiring 401-1 thru/or 401-3 in redundancy further again. For example, when the wiring 401-1 formed in the nonvolatile memory 34 interior thru/or 401-3 combine components, such as a transistor which constitutes nonvolatile memory 34, the path is compared, and even if it is linearly combinable, it is not formed linearly, but it is formed so that it may become predetermined die length. By doing in this way, wiring 401-1 thru/or the die length of 401-3 turn into die length more than die length required originally, and it will have big parasitic capacitance as compared with the case of the shortest die length required for wiring.

[0281] The circuit (built in the adapter 26 as a semiconductor IC) of the dedication currently designed in order to read data from nonvolatile memory 34 can read normally the data which nonvolatile memory 34 has memorized by setting up the impedance matched with the parasitic capacitance. However, if a probe is connected to wiring 401-1 thru/or 401-3 in order to read the data memorized by nonvolatile memory 34, it will become difficult for the parasitic capacitance and the capacity of composition by the probe to influence, and to read data normally.

[0282] Although the case where the portable device 6 was used above as a record medium was explained as an example, this invention can be applied also when transferring or copying data to other record media.

[0283] Moreover, contents can also be used as image data and other data in addition to musical-sound data, such as data of music, or voice data.

[0284] As mentioned above, according to this invention, the following effectiveness can be done so.

[0285] (1) Since this cannot be decoded even if it copies the contents currently recorded on HDD21, since it was made to record on HDD21 after also enciphering a cryptographic key with the key for preservation while enciphering to HDD21 and recording data, it can prevent that a duplicate is distributed in large quantities.

[0286] (2) Since the music and sound recording time were registered on the music database in order to carry out as [copy / between fixed time amount (in the case of the above-mentioned example 48 hours) / the music] when predetermined music was copied once, the count of a copy can be restricted and it can prevent distributing a duplicate in large quantities.

[0287] Since the hash value of data is calculated whenever it furthermore updates a database, and it was made to save, it becomes easy to prevent the alteration of a database.

[0288] (3) Since the contents on HDD21 were eliminated when passing contents to external equipment, it is prevented that the contents which are the original digital data all distribute the duplicate in large quantities in HDD21.

[0289] (4) Since a music database is formed in HDD21 and the whole hash value was checked each time, though the data which backed up the contents of HDD21 just before MUBU, and backed up

immediately after MUBU were restored to HDD21, it becomes possible to eliminate the data of delivery origin certainly.

[0290] (5) Since it was made to perform mutual recognition processing before that when a personal computer 1 passed data to an external device, what passes data to an inaccurate device is prevented.

[0291] (6) Since it checked by mutual recognition whether the software of a personal computer 1 would be just before passing data from an external instrument to a personal computer 1, what passes contents to inaccurate software is prevented.

[0292] (7) Since TOC was used when ISRC was used for the judgment of the identity of music and ISRC was not able to be acquired, it becomes possible to be able to acquire ISRC and to judge the identity of music as there being nothing.

[0293] (8) Since it does not know what kind of processing it has been as a whole only by analyzing the software of a personal computer 1 since it was made to make the adapter 26 by which external is carried out to a personal computer 1 pay a predetermined part among the software functions in a personal computer 1, what gives the function to alter and to mean software becomes difficult.

[0294] In addition, CPU11 may be made to perform processing which an adapter 26 performs by the secure program. In this case, the key for preservation which sets, for example, has the same value is generated by the contents manager 111 when the key for preservation is needed. Similarly, a hash value is concealed by the contents manager 111 and saved.

[0295] Moreover, when processing which an adapter 26 performs is performed by CPU11 by the secure program, a personal computer 1 is replaced with at the current time which RTC35 of an adapter 26 supplies, downloads the data of current time from the specific server (for example, EMD registration server 3) connected to the network 2, and performs processing of a judgment based on the current time. Moreover, when former time of day is set up with a predetermined time interval from the time of day which memorized current time and has been memorized, a personal computer 1 displays an error and you may make it not receive a setup of time of day in this case.

[0296] Although a series of processings mentioned above can also be performed by hardware, they can also be performed with software. When performing a series of processings with software, the program which constitutes the software is installed in a general-purpose personal computer etc. from a program storing medium possible [performing various kinds of functions] by installing the computer built into the hardware of dedication, or various kinds of programs.

[0297] The program storing medium which stores the program which is installed in a computer and made into the condition which can be performed by computer As shown in drawing 2 , a magnetic disk 41 (a floppy disk is included), an optical disk 42 (CD-ROM (Compact Disc-Read Only Memory) --) DVD (Digital Versatile Disc) is included. It is constituted by the package media which consist of a magneto-optic disk 43 (MD (Mini-Disc) is included) or semiconductor memory 44 or ROM12 in which a program is stored temporarily or permanently, HDD21, etc. Storing of the program to a program storing medium is performed through the interface of the communications department 25 etc. using the communication media of cables or wireless, such as the networks 2, such as a Local Area Network or the Internet, and digital satellite broadcasting, if needed.

[0298] In addition, in this specification, even if the processing serially performed in accordance with

the sequence that the step which describes the program stored in a program storing medium was indicated is not of course necessarily processed serially, it is a juxtaposition thing also including the processing performed according to an individual.

[0299] Moreover, in this specification, a system expresses the whole equipment constituted by two or more equipments.

[0300]

[Effect of the Invention] According to an information processor according to claim 1, the information processing approach according to claim 3, and the program storing medium according to claim 4, like the above Since other equipments judge whether the conditions of the utilization time of data can be satisfied and transferred data with the conditions of the utilization time of data based on the judgment result when transferring the data stored to other equipments After transferring data to other inaccurate equipments, data are copied to the equipment of further others and it becomes possible from the equipment to prevent certainly about data being reproduced unjustly.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the gestalt of 1 operation of the contents data management system concerning this invention.

[Drawing 2] It is drawing explaining the configuration of a personal computer 1.

[Drawing 3] It is drawing explaining the configuration of the portable device 6.

[Drawing 4] It is a block diagram explaining the configuration of the function of a personal computer 1.

[Drawing 5] It is drawing showing the example of a display operator guidance window.

[Drawing 6] The sound recording program 113 is drawing explaining the example of the window displayed on a display 20.

[Drawing 7] It is a flow chart explaining the processing in the case of copying contents to HDD21 from a compact disk.

[Drawing 8] It is a flow chart explaining term database check processing of step S12 of drawing 7 .

[Drawing 9] It is drawing showing the example of a term database.

[Drawing 10] It is drawing explaining a water mark.

[Drawing 11] It is drawing showing the example of a music database.

[Drawing 12] It is a flow chart explaining the actuation which moves contents to the portable device 6 from HDD21.

[Drawing 13] It is a flow chart explaining the actuation which moves contents to the portable device 6 from HDD21.

[Drawing 14] It is a flow chart explaining the actuation which moves contents to the portable device 6 from HDD21.

[Drawing 15] It is a flow chart explaining check processing of the playback conditions of contents

that step S55 of drawing 12 was chosen etc.

[Drawing 16] It is drawing explaining the playback conditions which the portable device 6 has managed.

[Drawing 17] It is a flow chart explaining the detail of format conversion processing of step S58 of drawing 12 .

[Drawing 18] It is a flow chart explaining the actuation in the case of copying contents to the portable device 6 from HDD21.

[Drawing 19] It is a flow chart explaining the actuation in the case of copying contents to the portable device 6 from HDD21.

[Drawing 20] It is a flow chart explaining the actuation in the case of copying contents to the portable device 6 from HDD21.

[Drawing 21] It is a flow chart explaining the actuation in the case of moving contents to HDD21 from the portable device 6.

[Drawing 22] It is an explanation flow chart about the actuation in the case of copying contents to HDD21 from the portable device 6.

[Drawing 23] It is a flow chart explaining the processing in the case of copying contents to HDD21 from the EMD server 4.

[Drawing 24] It is a flow chart explaining the detail of the processing about accounting of step S204 of drawing 23 .

[Drawing 25] It is drawing explaining an accounting log.

[Drawing 26] It is a flow chart explaining the processing in the case of copying contents to HDD21 from IEC60958 terminal 24a of the personal computer 1 of drawing 2 .

[Drawing 27] It is a flow chart explaining the processing in the case of copying contents to HDD21 from IEC60958 terminal 24a of the personal computer 1 of drawing 2 .

[Drawing 28] It is a flow chart explaining the actuation in the case of outputting contents to IEC60958 terminal 24a from HDD21.

[Drawing 29] It is a flow chart explaining the actuation in the case of outputting contents to IEC60958 terminal 24a from HDD21.

[Drawing 30] It is a flow chart explaining check processing of the playback conditions of step S275 of drawing 28 etc.

[Drawing 31] It is a flow chart explaining the actuation in the case of outputting contents by portable device 6 course from HDD21.

[Drawing 32] It is a flow chart explaining the actuation in the case of outputting contents by portable device 6 course from HDD21.

[Drawing 33] It is drawing explaining the function of nonvolatile memory 34.

[Drawing 34] It is a flow chart explaining actuation of an adapter 26.

[Drawing 35] It is drawing showing the configuration inside an adapter 26.

[Drawing 36] It is drawing showing the example of a configuration inside nonvolatile memory 34.

[Drawing 37] It is drawing showing the example of a configuration inside nonvolatile memory 34.

[Description of Notations]

1 Personal Computer 2 Network, 3 An EMD registration server, 6-1, or 6-3 portable device 11 CPU, 12 ROM 13RAM 21 HDD 24 A voice-input/output interface, 24a IEC60958 terminal 26 adapter 32 CPU 33 RAM 34 Nonvolatile memory, 35 RTC 36 ROM, 41 Magnetic disk 42 An optical disk and 43 magneto-optic disk 44 Semiconductor memory, 53 CPU 54 RAM and 55 ROM 59 DSP 61 flash memory 111 Contents manager 112 Display operator guidance program 113 Sound recording program 114 Contents database 131 An EMD selection program, 132 Check-in/check-out manager, 133 Copy manager 134 migration manager 135 A cipher system conversion program, 136 Compression method conversion program 137 Encryption program 138 compression / elongation program 139 Use condition conversion program 140 use condition manager 141 An authentication program, 142 A decode program, 143 The driver for PD, 144 Program for purchase 145 Program for purchase 181 Filtering data file 182 Display data file 183 Image file 184 Hysteresis data file 351 Protection aluminum layer 352 power-source pattern 401-1 thru/or 401-3 wiring

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-305855
(P2000-305855A)

(43) 公開日 平成12年11月2日 (2000.11.2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4

審査請求 未請求 請求項の数 4 O L (全 37 頁)

(21) 出願番号 特願2000-39261(P2000-39261)
(22) 出願日 平成12年2月17日 (2000.2.17)
(31) 優先権主張番号 特願平11-39223
(32) 優先日 平成11年2月17日 (1999.2.17)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72) 発明者 河上 達
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72) 発明者 石黒 隆二
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(74) 代理人 100082131
弁理士 稲本 義雄

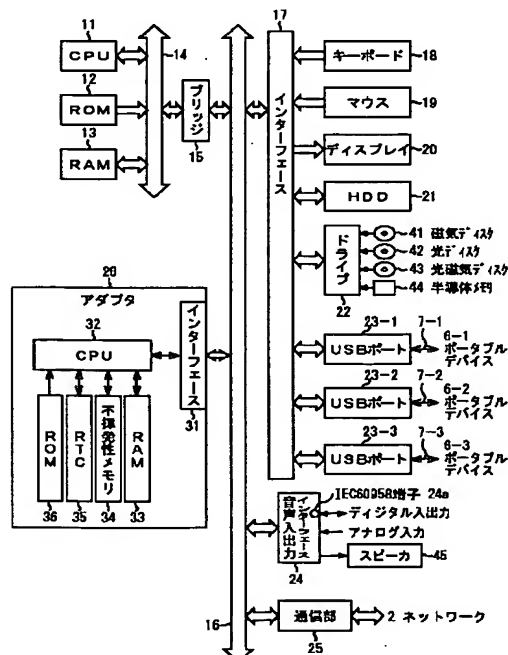
最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、並びにプログラム格納媒体

(57) 【要約】

【課題】 データが不正に複製されることを確実に防止できるようにする。

【解決手段】 CPU 11は、HDD 21に記録されている音楽データをポータブルデバイス6のフラッシュメモリに転送し、記憶させるとき、ポータブルデバイス6が、その音楽データについて付加されている再生条件、再生時課金条件、コピー条件などの各種の条件を守る機能を有しているか否かを判定し、各種条件を守る機能を有している場合にのみ、その音楽データをフラッシュメモリに転送し、記憶させる。



パーソナルコンピュータ 1

【特許請求の範囲】

【請求項 1】 データを蓄積する蓄積手段と、
前記蓄積手段に蓄積されている前記データの利用時の条件を保持する保持手段と、
前記蓄積手段に蓄積されている前記データを他の装置に移転するとき、前記他の装置が、前記データの利用時の条件を充足できるか否かを判定する判定手段と、
前記判定手段の判定結果に基づいて、前記蓄積手段に蓄積されている前記データを、前記保持手段に保持されている前記データの利用時の条件とともに、前記他の装置に移転する移転手段とを含むことを特徴とする情報処理装置。

【請求項 2】 前記データの利用時の条件は、再生制限条件、再生時課金条件、またはコピー制限条件を含むことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 データを蓄積する蓄積ステップと、
前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、
前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、前記他の装置が、前記データの利用時の条件を充足できるか否かを判定する判定ステップと、
前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを、前記保持ステップの処理で保持された前記データの利用時の条件とともに、前記他の装置に移転する移転ステップとを含むことを特徴とする情報処理方法。

【請求項 4】 データを蓄積する蓄積ステップと、
前記蓄積ステップの処理で蓄積された前記データの利用時の条件を保持する保持ステップと、
前記蓄積ステップの処理で蓄積された前記データを他の装置に移転するとき、
前記他の装置が、前記データの利用時の条件を充足できるか否かを判定する判定ステップと、
前記判定ステップでの判定結果に基づいて、前記蓄積ステップの処理で蓄積された前記データを、前記保持ステップの処理で保持された前記データの利用時の条件とともに、前記他の装置に移転する移転ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、蓄積されているデータを移転する場合にも、確実に、その不正な複製を防止することができるようにした、情報処理装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種のデータがデジタル

的に記録媒体に記録または再生されるようになってきた。その結果、複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが可能となってきた。

【0003】

【発明が解決しようとする課題】しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

【0004】(1) 例えば、コンパクトディスク(CD)からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができてしまう。

【0005】(2) CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピーの回数に制限がないため、複製が大量に配布されてしまう。

【0006】(3) パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、ポータブルデバイスなどの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

【0007】(4) 上記した(3)の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように(いわゆる、音楽データをムーブするように)パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば、ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

【0008】(5) パーソナルコンピュータが、ハードディスク内のデジタル音楽データをポータブルデバイスなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

【0009】(6) ポータブルデバイスなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御しているソフトウェアがどのようなソフトウェアであるかを確認しないため、違法なソフトウェアに対してデジタル音楽データが渡されてしまう恐れがある。

【0010】(7) CDより再生された音楽データをパーソナルコンピュータで取り扱うとき、複数の曲が同一か否かを判断するために、曲データに含まれるISRC(International Standard Recording Code)を使用することが可能であるが、CDによっては、ISRCデータを含んでいないものがある。この場合、複数の曲が同一であるか

否かを判定することができなくなる。

【0011】(8) 以上のような各機能は、パーソナルコンピュータ上で、ソフトウェアの制御により実現されるため、そのソフトウェアが改竄されると、システムの作成者が意図しない動作を行わせることができてしまう。

【0012】本発明はこのような状況に鑑みてなされたものであり、ハードディスクに記録されている音楽データが、不正な外部の機器に転送され、利用されることを防止するようにするものである。

【0013】

【課題を解決するための手段】請求項1に記載の情報処理装置は、データを蓄積する蓄積手段と、蓄積手段に蓄積されているデータの利用時の条件を保持する保持手段と、蓄積手段に蓄積されているデータを他の装置に移転するとき、他の装置が、データの利用時の条件を充足できるか否かを判定する判定手段と、判定手段の判定結果に基づいて、蓄積手段に蓄積されているデータを、保持手段に保持されているデータの利用時の条件とともに、他の装置に移転する移転手段とを含むことを特徴とする。

【0014】データの利用時の条件は、再生制限条件、再生時課金条件、またはコピー制限条件を含むようにすることができる。

【0015】請求項3に記載の情報処理方法は、データを蓄積する蓄積ステップと、蓄積ステップの処理で蓄積されたデータの利用時の条件を保持する保持ステップと、蓄積ステップの処理で蓄積されたデータを他の装置に移転するとき、他の装置が、データの利用時の条件を充足できるか否かを判定する判定ステップと、判定ステップでの判定結果に基づいて、蓄積ステップの処理で蓄積されたデータを、保持ステップの処理で保持されたデータの利用時の条件とともに、他の装置に移転する移転ステップとを含むことを特徴とする。

【0016】請求項4に記載のプログラム格納媒体のプログラムは、データを蓄積する蓄積ステップと、蓄積ステップの処理で蓄積されたデータの利用時の条件を保持する保持ステップと、蓄積ステップの処理で蓄積されたデータを他の装置に移転するとき、他の装置が、データの利用時の条件を充足できるか否かを判定する判定ステップと、判定ステップでの判定結果に基づいて、蓄積ステップの処理で蓄積されたデータを、保持ステップの処理で保持されたデータの利用時の条件とともに、他の装置に移転する移転ステップとを含むことを特徴とする。

【0017】請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載のプログラム格納媒体においては、蓄積されているデータを他の装置に移転するとき、他の装置が、データの利用時の条件を充足できるか否かが判定され、その判定結果に基づいて、データが他の装置に、データの利用時の条件と

もに移転される。

【0018】

【発明の実施の形態】図1は、本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。パーソナルコンピュータ1は、ローカルエリアネットワークまたはインターネットなどから構成されるネットワーク2に接続されている。パーソナルコンピュータ1は、EMD (Electrical Music Distribution) サーバ4-1乃至4-3から受信した、または後述するCD (Compact Disc) から読み取った楽音のデータ (以下、コンテンツと称する) を、所定の圧縮の方式 (例えば、ATRAC3 (商標)) に変換するとともにDES (Data Encryption Standard) などの暗号化方式で暗号化して記録する。

【0019】パーソナルコンピュータ1は、暗号化して記録しているコンテンツに対応して、コンテンツの利用条件を示す利用条件のデータを記録する。

【0020】利用条件のデータは、例えば、その利用条件のデータに対応するコンテンツを同時に利用することができるポータブルデバイス (Portable Device (PDとも称する)) の台数 (後述する、いわゆるチェックアウトできるPDの台数) を示す。利用条件のデータに示される数だけコンテンツをチェックアウトしたときでも、パーソナルコンピュータ1は、そのコンテンツを再生できる。

【0021】または、利用条件のデータは、コピーすることができることを示す。コンテンツをポータブルデバイス6-1乃至6-3にコピーしたとき、パーソナルコンピュータ1は記録しているコンテンツを再生できる。コンテンツの、ポータブルデバイス6-1乃至6-3に記憶させることができる回数は、制限される場合がある。この場合、コピーできる回数は、増えることがない。

【0022】または、利用条件のデータは、他のパーソナルコンピュータに移動することができるなどを示す。ポータブルデバイス6-1乃至6-3にコンテンツを移動させた後、パーソナルコンピュータ1が記録しているコンテンツは使用できなくなる (コンテンツが削除されるか、または利用条件が変更されて使用できなくなる)。

【0023】利用条件のデータの詳細は、後述する。

【0024】パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ (例えば、曲名、または再生条件など) と共に、USB (Universal Serial Bus) ケーブル7-1を介して、接続されているポータブルデバイス6-1に記憶させるとともに、ポータブルデバイス6-1に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する (以下、チェックアウトと称する)。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応す

る利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0025】パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-2を介して、接続されているポータブルデバイス6-2に記憶させるとともに、ポータブルデバイス6-2に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-3を介して、接続されているポータブルデバイス6-3に記憶させるとともに、ポータブルデバイス6-3に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【0026】また、パーソナルコンピュータ1は、USBケーブル7-1を介して、接続されているポータブルデバイス6-1にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-1に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する（以下、チェックインと称する）。より詳細には、チェックインしたとき、パーソナルコンピュータ1が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1増やされる。

【0027】パーソナルコンピュータ1は、USBケーブル7-2を介して、接続されているポータブルデバイス6-2にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-2に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、USBケーブル7-3を介して、接続されているポータブルデバイス6-3にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-3に消去させて（または、使用できなくさせて）、消去させたコンテンツに対応する利用条件のデータを更新する。

【0028】パーソナルコンピュータ1は、図示せぬ他のパーソナルコンピュータがポータブルデバイス6-1にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-2にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-3にチェックアウトしたコンテンツをチェックインできない。

【0029】EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3からコンテンツの

取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

【0030】EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。

【0031】EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【0032】WWW (World Wide Web) サーバ5-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD（例えば、CDのアルバム名、またはCDの販売会社など）、およびCDから読み取ったコンテンツに対応するデータ（例えば、曲名、または作曲者名など）をパーソナルコンピュータ1に供給する。WWWサーバ5-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD、およびCDから読み取ったコンテンツに対応するデータをパーソナルコンピュータ1に供給する。

【0033】ポータブルデバイス6-1は、パーソナルコンピュータ1から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を、コンテンツに関連するデータ（例えば、曲名、または再生制限など）と共に記憶する。ポータブルデバイス6-1は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。

【0034】例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。

【0035】使用者は、コンテンツを記憶したポータブ

ルデバイス6-1をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

【0036】ポータブルデバイス6-2は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-2は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-2をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

【0037】ポータブルデバイス6-3は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-3は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドホンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-3をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドホンなどで聴くことができる。

【0038】以下、ポータブルデバイス6-1乃至6-3を個々に区別する必要がないとき、単にポータブルデバイス6と称する。

【0039】図2は、パーソナルコンピュータ1の構成を説明する図である。CPU (Central Processing Unit) 11は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System)を実際に実行する。ROM (Read-only Memory) 12は、一般的には、CPU11が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 13は、CPU11の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成されるホストバス14により相互に接続されている。

【0040】ホストバス14は、ブリッジ15を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス16に接続されている。

【0041】キーボード18は、CPU11に各種の指令を入力するとき、使用者により操作される。マウス19は、ディスプレイ20の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ20は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21は、ハードディスクを駆動し、それらにCPU11によって実行するプログラムや情報を記録または再生させる。

【0042】ドライブ22は、装着されている磁気ディスク41、光ディスク42 (CDを含む)、光磁気ディスク43、または半導体メモリ44に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース17、外部バス16、ブリッジ15、およびホストバス14を介して接続されているRAM13に供給する。

【0043】USBポート23-1には、USBケーブル7-1を介して、ポータブルデバイス6-1が接続される。USBポート23-1は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-1のコマンドなどを含む）をポータブルデバイス6-1に出力する。

【0044】USBポート23-2には、USBケーブル7-2を介して、ポータブルデバイス6-2が接続される。USBポート23-2は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-2のコマンドなどを含む）をポータブルデバイス6-2に出力する。

【0045】USBポート23-3には、USBケーブル7-3を介して、ポータブルデバイス6-3が接続される。USBポート23-3は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD21、CPU11、またはRAM13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-3のコマンドなどを含む）をポータブルデバイス6-3に出力する。

【0046】IEC (International Electrotechnical Commission) 60958端子24aを有する音声入出力インタフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ45は、音声入出力インタフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【0047】これらのキーボード18乃至音声入出力インタフェース24は、インターフェース17に接続されており、インターフェース17は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0048】通信部25は、ネットワーク2が接続され、CPU11、またはHDD21から供給されたデータ（例えば、登録の要求、またはコンテンツの送信要求など）を、所定の方式のバケットに格納して、ネットワーク2を介して、送信するとともに、ネットワーク2を介して、受信したバケットに格納されているデータ（例えば、認証鍵、またはコンテンツなど）をCPU11、RAM1

3、またはHDD2 1に出力する。

【0049】半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ26のCPU32は、外部バス16、ブリッジ15、およびホストバス14を介してパーソナルコンピュータ1のCPU11と共働し、各種の処理を実行する。RAM33は、CPU32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC(Real Time Clock)35は、計時動作を実行し、時刻情報を提供する。

【0050】通信部25およびアダプタ26は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0051】以下、USBポート23-1乃至23-3を個々に区別する必要がないとき、単に、USBポート23と称する。以下、USBケーブル7-1乃至7-3を個々に区別する必要がないとき、単にUSBケーブル7と称する。

【0052】次に、ポータブルデバイス6の構成を図3を参照して説明する。電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU53乃至表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

【0053】USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1から転送されたコンテンツを含むデータを、内部バス58を介して、CPU53に供給する。

【0054】パーソナルコンピュータ1から転送されるデータは、1パケット当たり64バイトのデータから構成され、12Mbit/secの転送レートでパーソナルコンピュータ1から転送される。

【0055】ポータブルデバイス6に転送されるデータは、ヘッダおよびコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されていると共に、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、および再生回数カウンタなどが格納されている。コンテンツは、ATRAC3などの符号化方式で符号化され、暗号化されている。

【0056】ヘッダサイズは、ヘッダのデータ長(例えば、33バイトなど)を表し、ファイルサイズは、コンテンツのデータ長(例えば、33,636,138バイトなど)を表す。

【0057】コンテンツ鍵は、暗号化されているコンテ

ンツを復号するための鍵であり、パーソナルコンピュータ1とポータブルデバイス6との相互認証の処理で生成されたセッション鍵(一時鍵)を基に暗号化された状態で、パーソナルコンピュータ1からポータブルデバイス6に送信される。

【0058】ポータブルデバイス6がUSBケーブル7を介してパーソナルコンピュータ1のUSBポート23に接続されたとき、ポータブルデバイス6とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス6のDSP59は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読(復号)の処理を実行する。

【0059】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ1が生成するある値(チャレンジ)に対して、ポータブルデバイス6がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値(レスポンス)で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ1が生成する値は認証の処理毎に毎回変化するもので、例えば、ポータブルデバイス6が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ1は不正を検出できる。

【0060】コンテンツIDは、コンテンツに対応した、コンテンツを特定するためのIDである。

【0061】コーデックIDは、コンテンツの符号化方式に対応したIDであり、例えば、コーデックID"1"は、ATRAC3に対応し、コーデックID"0"は、MP3(MPEG(Moving Picture Experts Group) Audio Layer-3)に対応する。

【0062】ファイル名は、コンテンツに対応するパーソナルコンピュータ1が記録しているコンテンツファイル(後述する)をASCII(American National Standard Code for Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、または作曲者名などをASCIIコードに変換したデータである。

【0063】再生制限データは、コンテンツの再生が可能な期間(すなわち、開始日時または終了日時)または回数制限(再生の回数の制限)が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、"1"が割り当てられ、再生が可能な期間が設定されているとき、"2"が割り当てられ、回数制限および再生が可能な期間がいずれも設定されていないとき(いわゆる、買い取りで購入されたとき)、"0"が割り当てられる。

【0064】開始日時および終了日時は、再生制限データが"2"であるとき、再生可能期間の範囲を示すデー

10

20

30

40

50

タである。例えば、開始日時が“00040F”であり、終了日時が“00070F”であるとき、対応するコンテンツは、2000年4月15日から2000年7月15日まで、再生が可能である。

【0065】同様に、回数制限および再生回数カウンタは、再生制限データが“1”または“2”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が“02”であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが“01”であるとき、そのコンテンツが再生された回数は1回である。

【0066】例えば、再生制限データが“2”であり、開始日時が“00040F”であり、終了日時が“00070F”であり、回数制限が“02”であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間において、1日2回ずつ繰り返し再生できる。

【0067】例えば、再生制限データが“1”であり、開始日時が“000000”であり、終了日時が“000000”であり、回数制限が“0a”であり、再生回数カウンタが“05”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

【0068】ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツと共にコンテンツの書き込み命令を受信した場合、ROM55からRAM54に読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

【0069】フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【0070】なお、フラッシュメモリ61は、ポータブルデバイス6にメモリカードとして着脱可能とすることができる。

【0071】使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードとコンテンツとを読み出させ、DSP59に転送させる。

【0072】DSP59は、フラッシュメモリ61から転送された再生用コードに基づいてコンテンツをCRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生

して、再生したデータ(図3中においてD1で示す)をディジタル/アナログ変換回路63に供給する。

【0073】DSP59は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発信子59AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びにフレーム単位のLチャンネルクロックLCLK、およびRチャンネルクロックRCLKからなる動作クロックLRCLKをディジタルアナログ変換回路63に供給する。

【0074】DSP59は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路63に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

【0075】同様に、CPU53およびUSBコントローラ57も、水晶でなる発振子53Aまたは57Aがそれぞれ外付けされ、発振子53Aまたは57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

【0076】このように構成することで、ポータブルデバイス6は、CPU53、DSP59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化すると共に小型化することができる。

【0077】ディジタルアナログ変換回路63は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路64に供給する。増幅回路64は、音声信号を増幅して、ヘッドフォンジャック65を介して、図示せぬヘッドフォンに音声信号を供給する。

【0078】このように、ポータブルデバイス6は、図示せぬ再生/停止ボタンが押圧操作されたとき、CPU53の制御に基づいてフラッシュメモリ61に記憶されているコンテンツを再生するとともに、再生中に再生/停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【0079】ポータブルデバイス6は、停止後に再度再生/停止ボタンが押圧操作されたとき、CPU53の制御に基づいて停止した位置からコンテンツの再生を再開する。再生/停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス6は、自動的に電源をオフして消費電力を低減する。

【0080】因みに、ポータブルデバイス6は、電源がオフになった後に再生/停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1曲目から再生する。

【0081】また、ポータブルデバイス6のCPU53は、LCDコントローラ68を制御して、表示部67に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量および乾電池51の残量等の情報を表示させる。

【0082】さらに、ポータブルデバイス6は、EEPROM68に、フラッシュメモリ80に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ61のブロック位置、およびその他の種々のメモリ蓄積情報等のいわゆるFAT（File Allocation Table）を格納する。

【0083】因みに、本実施の形態においては、コンテンツは、64KByteを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がFATに格納される。

【0084】フラッシュメモリ61にFATが格納される場合、例えば、1曲目のコンテンツがCPU53の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

【0085】このように、FATは、フラッシュメモリ61へのコンテンツの書き込みの度に書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

【0086】FATがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書き換えの回数に達してしまい、フラッシュメモリ61の書き換えができなくなってしまう。

【0087】そこで、ポータブルデバイス6は、FATをEEPROM68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書き換えの頻度を少なくしている。

【0088】書き換えの回数の多いFATをEEPROM68に記憶させることにより、FATをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU53は、EEPROM68にFATを追記するように書き込ませるので、EEPROM68の同一の領域の書き換えの頻度を少なくして、EEPROM68が短期間で書き換え不能になることを防止する。

【0089】ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき

（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

【0090】ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

【0091】CPU53は、USB接続されたとき、DSP59のコンテンツの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【0092】このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

【0093】なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

【0094】図4は、CPU11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、暗号方式変換プログラム135、圧縮方式変換プログラム136、暗号化プログラム137、利用条件変換プログラム139、利用条件管理プログラム140、認証プログラム141、復号プログラム142、PD用ドライバ143、購入用プログラム144、および購入用プログラム145などの複数のプログラムで構成されている。

【0095】コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0096】EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、後述するEMDの登録の処理において、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4-1乃

至4-3のいずれかとの接続を選択して、購入用アプリケーション115、または購入用プログラム144若しくは142に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0097】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの設定、およびコンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトするか、またはポータブルデバイス6-1乃至6-3に記憶されているコンテンツをチェックインする。

【0098】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新する。

【0099】コピー管理プログラム133は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにコピーするか、またはポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114にコピーする。

【0100】移動管理プログラム134は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかに移動するか、またはポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114に移動する。

【0101】暗号方式変換プログラム135は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの暗号化の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの暗号化の方式、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの暗号化の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の暗号化の方式に変換する。

【0102】また、暗号方式変換プログラム135は、ポータブルデバイス6-1または6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス6-1または6-3が利用可能な暗号化方式に変換する。

【0103】圧縮方式変換プログラム136は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの圧縮の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの圧縮の方式、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの圧縮の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の圧縮の方式に変換する。

【0104】また、圧縮方式変換プログラム136は、ポータブルデバイス6-1または6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス6-1または6-3が利用可能な圧縮の方式に変換する。

【0105】暗号化プログラム137は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【0106】圧縮／伸張プログラム138は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム138は、符号化されているコンテンツを伸張（復号）する。

【0107】利用条件変換プログラム139は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの利用条件を示すデータ、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース114が記録している利用条件ファイル162-1乃至162-Nに格納されている利用条件データと同一のフォーマットに変換する。

【0108】また、利用条件変換プログラム139は、ポータブルデバイス6-1または6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス6-1または6-3が利用可能な利用条件のデータに変換する。

【0109】利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理を実行する前に、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至

162-Nに格納されている利用条件のデータに対応するハッシュ値(後述する)を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム140は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理に伴う、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

【0110】認証プログラム141は、コンテンツ管理プログラム111と購入用アプリケーションプログラム115との相互認証の処理、およびコンテンツ管理プログラム111と購入用プログラム144との相互認証の処理を実行する。また、認証プログラム141は、EMDサーバ4-1と購入用アプリケーションプログラム115との相互認証の処理、EMDサーバ4-2と購入用プログラム144との相互認証の処理、およびEMDサーバ4-3と購入用プログラム145との相互認証の処理で利用される認証鍵を記憶している。

【0111】認証プログラム141が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされたとき、認証プログラム141に記憶されておらず、表示操作指示プログラム112により登録の処理が正常に実行されたとき、EMD登録サーバ3から供給され、認証プログラム141に記憶される。

【0112】復号プログラム142は、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツをパーソナルコンピュータ1が再生するとき、コンテンツを復号する。

【0113】PD用ドライバ143は、ポータブルデバイス6-2に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-2から所定のコンテンツをチェックインするとき、ポータブルデバイス6-2にコンテンツまたはポータブルデバイス6-2に所定の処理を実行させるコマンドを供給する。

【0114】PD用ドライバ143は、ポータブルデバイス6-1に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-1から所定のコンテンツをチェックインするとき、デバイスドライバ116-1にコンテンツ、またはデバイスドライバ116-1に所定の処理を実行させるコマンドを供給する。

【0115】PD用ドライバ143は、ポータブルデバイス6-3に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス6-3から所定のコンテンツをチェックインするとき、デバイスドライバ116-2にコンテンツ、またはデバイスドライバ116-2に所定の処理を実行させるコマンドを供給する。

【0116】購入用プログラム144は、いわゆる、ブ

ラグインプログラムであり、コンテンツ管理プログラム111と共にインストールされ、EMD登録サーバ3からネットワーク2を介して供給され、または所定のCDに記録されて供給される。購入用プログラム144は、パーソナルコンピュータ1にインストールされたとき、コンテンツ管理プログラム111の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム111とデータを送受信する。

【0117】購入用プログラム144は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる(例えば、使用者が、直接、購入用プログラム144を読み出しても、インストラクションを特定できないなど)ように構成されている。

【0118】購入用プログラム144は、ネットワーク2を介して、EMDサーバ4-2に所定のコンテンツの送信を要求するとともに、EMDサーバ4-2からコンテンツを受信する。また、購入用プログラム144は、EMDサーバ4-2からコンテンツを受信するとき、課金の処理を実行する。

【0119】購入用プログラム145は、コンテンツ管理プログラム111と共にインストールされるプログラムであり、ネットワーク2を介して、EMDサーバ4-3に所定のコンテンツの送信を要求するとともに、EMDサーバ4-3からコンテンツを受信する。また、購入用プログラム145は、EMDサーバ4-3からコンテンツを受信するとき、課金の処理を実行する。

【0120】表示操作指示プログラム112は、フィルタリングデータファイル181、表示データファイル182、画像ファイル183-1乃至183-K、または履歴データファイル184を基に、ディスプレイ20に所定のウィンドウの画像を表示させ、キーボード18またはマウス19への操作を基に、コンテンツ管理プログラム111にチェックインまたはチェックアウトなどの処理の実行を指示する。

【0121】フィルタリングデータファイル181は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD21に記録されている。

【0122】表示データファイル182は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツに対応するデータを格納して、HDD21に記録されている。

【0123】画像ファイル183-1乃至183-Kは、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに対応する画像、または後述するパッケージに対応する画像を格納

10

20

30

40

50

して、HDD2 1 に記録されている。

【0124】以下、画像ファイル183-1乃至183-Kを個々に区別する必要がないとき、単に、画像ファイル183と称する。

【0125】履歴データファイル184は、コンテンツデータベース114に記録されているコンテンツファイル161-1乃至161-Nに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD2 1 に記録されている。

【0126】表示操作指示プログラム112は、登録の処理のとき、ネットワーク2を介して、EMD登録サーバ3に、予め記憶しているコンテンツ管理プログラム111のIDを送信するとともに、EMD登録サーバ3から認証用鍵およびEMD選択プログラム131を受信して、コンテンツ管理プログラム111に認証用鍵およびEMD選択プログラム131を供給する。

【0127】録音プログラム113は、所定のウィンドウの画像を表示させて、キーボード18またはマウス19への操作を基に、ドライブ22に装着された光ディスク42であるCDからコンテンツの録音時間などのデータを読み出す。

【0128】録音プログラム113は、CDに記録されているコンテンツの録音時間などを基に、ネットワーク2を介して、WWWサーバ5-1または5-2にCDに対応するデータ（例えば、アルバム名、またはアーティスト名など）またはCDに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ5-1または5-2からCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを受信する。

【0129】録音プログラム113は、受信したCDに対応するデータまたはCDに記録されているコンテンツに対応するデータを、表示操作指示プログラム112に供給する。

【0130】また、録音の指示が入力されたとき、録音プログラム113は、ドライブ22に装着された光ディスク42であるCDからコンテンツを読み出して、コンテンツ管理プログラム111に出力する。

【0131】コンテンツデータベース114は、コンテンツ管理プログラム111から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル161-1乃至161-Nのいずれかに格納する（HDD2 1 に記録する）。コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nにそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル161-1乃至161-Nにそれぞれ対応する利用条件ファイル162-1乃至162-Nのいずれかに格納する（HDD2 1 に記録する）。

【0132】コンテンツデータベース114は、コンテンツファイル161-1乃至161-Nまたは利用条件ファイル162-1乃至162-Nをレコードとして記録してもよい。

【0133】例えば、コンテンツファイル161-1に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-1に格納されている。コンテンツファイル161-Nに格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル162-Nに格納されている。

【0134】なお、利用条件ファイル162-1乃至162-Nに記録されているデータは、後述する期限データベースに記録されているデータ、または曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース114は、後述する期限データベースおよび曲データベースを包含して、構成されている。

【0135】以下、コンテンツファイル161-1乃至161-Nを個々に区別する必要がないとき、単に、コンテンツファイル161と称する。以下、利用条件ファイル162-1乃至162-Nを個々に区別する必要がないとき、単に、利用条件ファイル162と称する。

【0136】購入用アプリケーションプログラム115は、EMD登録サーバ3からネットワーク2を介して供給され、または所定のCD-ROMに記録されて供給される。購入用アプリケーションプログラム115は、ネットワーク2を介して、EMDサーバ4-1に所定のコンテンツの送信を要求するとともに、EMDサーバ4-1からコンテンツを受信して、コンテンツ管理プログラム111に供給する。また、購入用アプリケーションプログラム115は、EMDサーバ4-1からコンテンツを受信するとき、課金の処理を実行する。

【0137】次に、表示データファイル82に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル161-1乃至161-Nとの対応付けについて説明する。

【0138】コンテンツファイル161-1乃至161-Nのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、またはフィルタリングパッケージのいずれかである。

【0139】オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4-1乃至4-3におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、または一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、または追加した情報の変更）することができる。

【0140】マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【0141】フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フ

ィルタリングデータは、EMDサーバ4-1乃至4-3またはWWWサーバ5-1若しくは5-2などからネットワーク2を介して供給され、または所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

【0142】フィルタリングデータは、所定のコンテンツを選択する、またはコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを

利用すれば、パーソナルコンピュータ1は、今週の日本のポップス1位のコンテンツ乃至今週の日本のポップス10位のコンテンツを特定することができる。

【0143】フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、または曲名に“愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

【0144】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ221（コンテンツ用表示データ221に使用者が設定したデータを含む）、または履歴データ184などと、フィルタリングデータとを対応させて選択される。

【0145】ドライバ117は、コンテンツ管理プログラム111などの制御の基に、音声入出力インターフェース24を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム111に供給するか、若しくはコンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツをデジタルデータとして出力するか、または、コンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツに対応するアナログ信号を出力する。

【0146】図5は、表示操作指示プログラム112を起動させたとき、操作指示プログラム112がディスプレイ20に表示させる表示操作指示ウィンドウの例を示す図である。

【0147】表示操作指示ウィンドウには、録音プログ

ラム113を起動させるためのボタン201、EMD選択プログラム131を起動させるためのボタン202、チェックインまたはチェックアウトの処理の設定を行うフィールドを表示させるためのボタン203、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン204等が配置されている。

【0148】ボタン205が選択されているとき、フィールド211には、オリジナルパッケージに対応するデータが表示される。ボタン206が選択されているとき、フィールド211には、マイセレクトパッケージに対応するデータが表示される。ボタン207が選択されているとき、フィールド211には、フィルタリングパッケージに対応するデータが表示される。

【0149】フィールド211に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、またはアーティスト名などである。

【0150】例えば、図5においては、パッケージ名称“ファースト”およびアーティスト名“A太郎”、およびパッケージ名称“セカンド”およびアーティスト名“A太郎”などがフィールド211に表示される。

【0151】フィールド212には、フィールド211で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド212に表示されるデータは、例えば、曲名、演奏時間、またはチェックアウト可能回数などである。

【0152】例えば、図5においては、パッケージ名称“セカンド”に対応するパッケージが選択されているので、パッケージ名称“セカンド”に対応するパッケージに属するコンテンツに対応する曲名“南の酒場”およびチェックアウト可能回数（例えば、8分音符の1つがチェックアウト1回に相当し、8分音符が2つでチェックアウト2回を示す）、並びに曲名“北の墓場”およびチェックアウト可能回数（8分音符が1つでチェックアウト1回を示す）などがフィールド212に表示される。

【0153】このように、フィールド212に表示されるチェックアウト可能回数としての1つの8分音符は、対応するコンテンツが1回チェックアウトできることを示す。

【0154】フィールド212に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が0である。（ただし、パーソナルコンピュータ1はそのコンテンツを再生することができる。））ことを示す。また、フィールド212に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限が無い（何度でも、チェックアウトできる）ことを示している。

【0155】なお、チェックアウト可能回数は、図5に示すように所定の図形（例えば、円、星、月などでもよ

い)の数で表示するだけでなく、数字等で表示してもよい。

【0156】また、表示操作指示ウィンドウには、選択されているパッケージまたはコンテンツに対応付けられている画像等(図4の画像ファイル183-1乃至183-Kのいずれかに対応する)を表示させるフィールド208が配置されている。ボタン209は、選択されているコンテンツを再生する(コンテンツに対応する音声スピーカー45に出力させる)とき、クリックされる。

【0157】ボタン205が選択され、フィールド211に、オリジナルパッケージに対応するデータが表示されている場合、フィールド212に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、選択されている曲名に対応する、コンテンツデータベース114に格納されている所定のコンテンツを消去させる。

【0158】録音プログラム113が表示させるウィンドウのボタン(後述するボタン255)が選択されて(アクティブにされて)いる場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツの曲名を表示するフィールド213を表示する。

【0159】録音プログラム113が表示させるウィンドウのボタンが選択されている場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、コンテンツデータベース114に記録した、CDから読み出したコンテンツを予め指定されているポータブルデバイス6-1乃至6-3のいずれかにチェックアウトさせる。

【0160】フィールド213にはコンテンツの曲名に対応させて、フィールド213の最も左に、そのコンテンツがパーソナルコンピュータ1にチェックインできるか否かを示す記号が表示される。例えば、フィールド213の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできる(すなわち、パーソナルコンピュータ1からチェックアウトされた)ことを示している。フィールド213の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできない(すなわち、パーソナルコンピュータ1からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた)ことを示している。

【0161】表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィン

ドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツが属するポータブルパッケージ(ポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツが属するパッケージ)の名称を表示するフィールド214、フィールド213を閉じるためのボタン210、およびチェックインまたはチェックアウトを実行させるボタン215を表示する。

【0162】更に、表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、フィールド212で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン216、フィールド213で選択された曲名に対応するコンテンツのチェックインを設定するボタン217、フィールド213に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン218、およびチェックインまたはチェックアウトの設定を取り消すボタン219を配置させる。

【0163】ボタン216乃至219の操作によるチェックインまたはチェックアウトの設定だけでは、パーソナルコンピュータ1は、チェックインまたはチェックアウトの処理を実行しない。

【0164】ボタン216乃至219の操作によるチェックインまたはチェックアウトの設定をした後、ボタン215がクリックされたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111にチェックインまたはチェックアウトの処理を実行させる。すなわち、ボタン215がクリックされたとき、表示操作指示プログラム112は、チェックインまたはチェックアウトの設定に基づき、コンテンツ管理プログラム111に、ポータブルデバイス6-1乃至6-3のいずれかにコンテンツを送信させるか、またはチェックインに対応する所定のコマンド(例えば、ポータブルデバイス6-1乃至6-3のいずれかが記憶している所定のコンテンツを消去させるコマンドなど)を送信させるとともに、送信したコンテンツまたはコマンドに対応する利用条件ファイル162に格納されている利用条件のデータを更新させる。

【0165】チェックインまたはチェックアウトが実行されたとき、表示操作指示プログラム112は、送信したコンテンツまたは送信されたコマンドに対応して、履歴データファイル184に格納されている履歴データを更新する。履歴データは、チェックインまたはチェックアウトされたコンテンツを特定する情報、またはそのコンテンツがチェックインまたはチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス6-1乃至6-3の名称などから成る。

【0166】チェックインまたはチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェック

10

20

30

40

50

インまたはチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックインまたはチェックアウトの処理の回数を減らして、チェックインまたはチェックアウトに必要な時間全体（設定および実行を含む）を短くすることができる。

【0167】図6は、録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。例えば、wwwサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド251に、"アシンクロナイズド"などのCDのタイトルを表示する。wwwサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド252に、例えば、"クワイ"などのアーティスト名を表示する。

【0168】wwwサーバ5-2から受信したCDの情報を基に、録音プログラム113は、フィールド253の曲名を表示する部分に、例えば、"ヒート"、"ブラネット"、"ブラック"、"ソウル"などの曲名を表示する。同様に、録音プログラム113は、フィールド253のアーティストを表示する部分に、例えば、"クワイ"などのアーティスト名を表示する。

【0169】録音プログラム113が所定のCDの情報を受信した後、録音プログラム113は、HDD21の所定のディレクトリにCDの情報を格納する。

【0170】ボタン254などがクリックされて、CDの情報の取得の指示を受けたとき、録音プログラム113は、始めに、HDD21の所定のディレクトリを検索する。録音プログラム113は、そのディレクトリにCDの情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されているCDの情報を利用するか否かを選択させる。

【0171】録音プログラム113が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン256がクリックされたとき、録音プログラム113は、ドライブ22に格納されているCDからコンテンツを読み出して、CDから読み出したコンテンツをCDの情報と共にコンテンツ管理プログラム111に供給する。コンテンツ管理プログラム111の圧縮/伸張プログラム138は、録音プログラム113から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム137は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム139は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

【0172】コンテンツ管理プログラム111は、圧縮され、暗号化されたコンテンツを利用条件のデータと共に、コンテンツデータベース114に供給する。

【0173】コンテンツデータベース114は、コンテンツ管理プログラム111から受信したコンテンツに対応するコンテンツファイル161および利用条件ファイル162を生成して、コンテンツファイル161にコン

テンツを格納するとともに、利用条件ファイル162に利用条件のデータを格納する。

【0174】コンテンツ管理プログラム111は、コンテンツデータベース114にコンテンツおよびコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム113から受信したCDの情報および利用条件のデータを表示操作指示プログラム112に供給する。

【0175】表示操作指示プログラム112は、録音の処理でコンテンツデータベース114に格納されたコンテンツに対応する利用条件のデータおよびCDの情報を基に、表示データファイル182に格納する表示用のデータを生成する。

【0176】録音プログラム113が表示させるウィンドウには、更に、CDから読み出したコンテンツをコンテンツデータベース114に記録したとき、自動的に、CDから読み出したコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトさせるか否かの設定を行うボタン255が配置されている。

【0177】例えば、ボタン255がクリックされたとき、録音プログラム113は、ポータブルデバイス6-1乃至6-3のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス6-1乃至6-3のいずれかを選択したとき、パーソナルコンピュータ1は、選択されたポータブルデバイス6-1乃至6-3のいずれかに、自動的に、CDから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから"チェックアウトしない"を選択した場合、パーソナルコンピュータ1は、CDからコンテンツを記録したとき、チェックアウトしない。

【0178】このように、録音プログラム113が表示させるウィンドウのボタン255をアクティブにしておくだけで、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、パーソナルコンピュータ1は、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに、CDから読み出したコンテンツをチェックアウトさせることができる。

【0179】次に、図7のフローチャートを参照して、コンテンツ管理プログラム111、表示操作指示プログラム112、録音プログラム113、およびコンテンツデータベース114を実行するCPU11による、ドライブ22に装着されたCDから再生したコンテンツをHDD21に転送し、コピーする場合の処理について説明する。使用者がキーボード18またはマウス19を操作して、インタフェース17を介してCPU11に対してドライブ22に装着されたCD（図示せず）から再生されたコンテンツをHDD21に転送、コピーする指令を入力すると、録音プログラム113は、ステップS11において、インタフェース17を介してディスプレイ20にコピーするコンテンツを選択するための、例えば、図6に示すGU

I (Graphical User Interface) を表示させる。

【0180】具体的には、例えば、録音プログラム113は、ドライブ22に装着されたCDのTOC (Table Of Contents) を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ20に表示させる。または、録音プログラム113は、CDに含まれている各コンテンツ毎のISRC (International Standard Recording Code) を読み出し、そのコンテンツの情報を得て、ディスプレイ20に表示させる。あるいはまた、ボタン254がクリックされたとき、録音プログラム113は、ネットワーク2を介してWWWサーバ5-1または5-2にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド253に表示させる。

【0181】使用者は、ディスプレイ20のGUIを利用してキーボード18またはマウス19を操作し、フィールド253に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

【0182】次に、ステップS12において、録音プログラム113は、利用条件管理プログラム140に、HDD21に格納されている期限データベース(図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する)をチェックさせる。この期限データベースチェック処理の詳細は、図8のフローチャートに示されている。

【0183】ステップS31において利用条件管理プログラム140は、アダプタ26のCPU32と共働して、期限データベース全体のハッシュ値を計算し、ステップS32において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0184】なお、期限データベースにデータが何ら記録されていないとき、利用条件管理プログラム140は、ハッシュ値を計算しない。

【0185】すなわち、HDD21には、期限データベースが形成されており、この期限データベースには、図9に示すように、HDD21に記録されているコンテンツ

(コンテンツ)を管理する管理情報として、過去に記録されたことのあるコンテンツのISRCとコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS38において、アダプタ26のCPU32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。

【0186】ハッシュ関数は、任意の長さのメッセージを固定長に短く圧縮した値にマップする一方向性の関数

であり、圧縮したデータからもとのデータを求める逆変換が困難な性質を持つものである。また、ハッシュ値同士の衝突が起こりにくく、即ち、例えば違う二つのメッセージに対して同じ値を付けることを困難にするものである。ハッシュ関数は、メッセージが通信途中で改竄されなかったことを確認するためのチェックサムとして用いられ、デジタル署名の中で用いられる。ハッシュ関数の例としては、SHA (Secure Hash Algorithm), MD (Message Digest) 5 などがある。

【0187】利用条件管理プログラム140は、ステップS31において、CPU32が実行したのと同様にハッシュ値を計算する。そして、ステップS32において、利用条件管理プログラム140は、CPU32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS31で、いま自分自身が計算したハッシュ値とを比較する。

【0188】ステップS33において、利用条件管理プログラム140は、ステップS31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム140は、ステップS34において、例えば、録音プログラム113に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インタフェース17を介してディスプレイ20に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されているコンテンツを再生し、HDD21にコピーする処理が禁止される。

【0189】ステップS31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS35に進み、利用条件管理プログラム140は、録音プログラム113に、ステップS11で指定されたコピーするコンテンツとして選択されたコンテンツ(選択されたコンテンツ)のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム140は、録音プログラム113に、そのCDのTOCのデータを読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

【0190】ステップS36において、利用条件管理プログラム140は、ステップS35で取得したISRC(すなわち、選択されたコンテンツ)が期限データベース(図9)に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD21に記録されていないことになるので、ステップS37に進み、利用条件管理プログラム140は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム140は、この現在の日時として、CPU32から転送を

受けた、アダプタ26のRTC35が出力する値を利用する。そして、ステップS38において、利用条件管理プログラム140は、その時点における期限データベースのデータを読み出し、アダプタ26のCPU32に転送する。CPU32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

【0191】次に、ステップS39において、利用条件管理プログラム140は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS13において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

【0192】ステップS36において、選択されたコンテンツのISRCが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、HDD21に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップS40に進み、利用条件管理プログラム140は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ26のRTC35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているもので、そのコンテンツを再度コピーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場合には、HDD21へのコピーが許容される。そこで、ステップS41に進み、利用条件管理プログラム140は、期限データベースの日時を、過去の登録日時から現在の日時（RTC35の出力する日時）に変更させる。そして、ステップS38に戻り、利用条件管理プログラム140は、再び、期限データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させるとともに、ステップS39において、そのコンテンツに対して未登録のフラグを設定する。

【0193】一方、ステップS40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択されたコンテンツのHDD21へのコピーが禁止される。そこで、この場合には、ステップS42に進み、利用条件管理プログラム140は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

【0194】ステップS40の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテ

ンツのコピーの生成を不当に妨げることなく、例えば、不正な販売または配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップS40においては、判定の基準は48時間以上の経過としたが、48時間に限らず、例えば、12時間乃至168時間のいずれかの時間であればよい。

【0195】以上のようにして、期限データベースチェック処理により、選択されたコンテンツがHDD21に登録されているか否かを表すフラグが設定される。

【0196】図7に戻り、ステップS13においてコピー管理プログラム133は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップS14に進み、コピー管理プログラム133は、録音プログラム113に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ20に表示させる。これにより、使用者は、そのコンテンツをHDD21にコピーすることができない理由を知ることができる。

【0197】ステップS13において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップS15に進み、録音プログラム113は、ドライブ22を制御し、そこに装着されているCDからコンテンツを読み出させる。このコンテンツには、図10に示すように、所定の位置にウォータマークコードが挿入されている。録音プログラム113は、ステップS16において、コンテンツに含まれているウォータマークコードを抽出し、そのウォータマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS18に進み、コピー管理プログラム133は、録音プログラム113に例えば、「コピーは禁止されています」のようなメッセージをインタフェース17を介してディスプレイ20に表示させ、コピー処理を終了させる。

【0198】これに対して、ステップS17において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS19に進み、録音プログラム113は、コンテンツを、圧縮/伸張プログラム138に、例えば、ATRAC (Adaptive Transform Acoustic Coding) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップS20において、録音プログラム113は、暗号化プログラム137に、予め設定され、メモリ13に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encryption Algorithm) 方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ26のCPU32により発生させた乱数に基づいて生成したも

のを用いることもできる。このように、パーソナルコンピュータ 1 だけではなく、それに付随して装着されたハードウェアとしてのアダプタ 26 の CPU 32 と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【0199】次に、ステップ S 21 において、録音プログラム 113 は、暗号化されたデータを、コンテンツデータベース 114 に転送し、1つのファイル（コンテンツファイル 161 として）としてファイル名を付けて HDD 21 に保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報（例えば、先頭からのバイト数）を与えて保存するようにしてもよい。

【0200】この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【0201】さらに、ステップ S 22 において、録音プログラム 113 は、暗号化プログラム 137 に、予め定められている不揮発性メモリ 34 に記憶されている保存用鍵を使って、上述した DES 方式、FEAL 方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、HDD 21 の曲データベース（図 4 に示すコンテンツデータベース 114 の利用条件ファイル 162-1 乃至 162-N に対応する）に保存する。

【0202】ステップ S 23 において、録音プログラム 113 は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者が GUI を介して入力した曲名の情報の要素を組にして HDD 21 の曲データベースに登録する（利用条件ファイル 162-1 乃至 162-N として記録する）。そして、ステップ S 24 において、録音プログラム 113 は、CPU 32 に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ 34 に保存させる。

【0203】このようにして、例えば、図 11 に示すような曲データベースが、HDD 21 上に登録される。この例においては、アイテム 1 乃至アイテム 3 のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件（開始日時、終了日時、回数制限）、再生回数カウンタ、再生時課金条件、コピー条件（回数）、コピー回数カウンタ、およびコピー条件（SCMS）が記録されている。

【0204】例えば、SDMI（Secure Digital Music Initiative）が規定する方式では、CD からコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、3 回に設定される。

【0205】CD から HDD 21 にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ 1 が故障して、HDD 2

1 に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD 21 に記録することができる。

【0206】また、例えば、ネットワーク 2 を介して HDD 21 に記録されている期限データベースの内容を共有することもできる。

【0207】以上においては、ISRC に対応して複製された日時が記憶されている場合を例として説明したが、コンテンツや CD を識別する情報であれば、他のもの（例えば、曲名、アルバム名、それらの組み合わせなど）を利用することもできる。

【0208】次に、図 12 乃至図 14 のフローチャートを参照して、表示操作指示プログラム 112 およびコンテンツ管理プログラム 111 を実行する CPU 11 およびメインプログラムを実行する CPU 52 による、HDD 21 からポータブルデバイス 6 のフラッシュメモリ 61（例えば、メモリスティック（商標））に、コンテンツを移動する処理およびチェックアウトの処理について説明する。

【0209】始めに、コンテンツの移動の処理について説明する。ステップ S 51 において、移動管理プログラム 134 は、利用条件管理プログラム 140 に、曲データベース全体のハッシュ値を計算させ、ステップ S 52 で、前回 CPU 32 に計算させ、不揮発性メモリ 34 に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム 134 は、ステップ S 53 に進み、表示操作指示プログラム 112 に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ 20 に表示させた後、処理を終了させる。この場合の処理は、図 8 のステップ S 31 乃至ステップ S 34 の処理と同様の処理である。この場合においては、HDD 21 からポータブルデバイス 6 へのコンテンツの移動が実行されないことになる。

【0210】次に、ステップ S 54 において、移動管理プログラム 134 は、HDD 21 に形成されている曲データベース（コンテンツデータベース 114 に含まれる）から、そこに登録されているコンテンツの情報を読み出し、表示操作指示プログラム 112 に、選択のための GUI としてディスプレイ 20 に表示させる。使用者は、この選択のための GUI に基づいて、HDD 21 からポータブルデバイス 6 へ移動させるコンテンツを、図 5 のフィールド 212 に表示される曲名、ボタン 216 などをクリックして選択する。次に、ステップ S 55 において、移動管理プログラム 134 は、ステップ S 54 で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図 15 のフローチャートを参照して後述する。

【0211】次に、ステップ S 56 において、パーソナルコンピュータ 1 の認証プログラム 141 とポータブルデバイス 6 の CPU 53 との間において、相互認証処理が

行われ、通信用鍵が共有される。

【0212】例えば、ポータブルデバイス6のフラッシュメモリ61（または、EEPROM68）には、マスター鍵KMが予め記憶されており、パーソナルコンピュータ1のRAM13（または、HDD21の所定のファイル）には、個別鍵KPとIDが予め記憶されているものとする。CPU53は、認証プログラム141から、RAM13に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMとハッシュ関数を適用して、RAM13に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1とポータブルデバイス6の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0213】あるいはまた、パーソナルコンピュータ1のRAM13にIDとマスター鍵KMPを予め記憶させておくとともに、ポータブルデバイス6のフラッシュメモリ61にもポータブルデバイス6のIDとマスター鍵KMを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【0214】なお、認証の方法としては、例えば、IOS（International Organization for Standardization）9798-2を利用することができる。

【0215】相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS57において、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図7のステップS20の処理で暗号化されている）をHDD21から読み出す。ステップS58において、移動管理プログラム134は、ステップS57で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップS19の処理）、暗号化方式（ステップS20の処理）、フォーマット（例えば、ヘッダの方式など）などをポータブルデバイス6のものに変換する処理を実行する。この変換処理の詳細は、図17のフローチャートを参照して後述する。

【0216】ステップS59において、移動管理プログラム134は、PD用ドライバ143に、ステップS58で変換したコンテンツを、USBポート23を介してポータブルデバイス6に転送させる。ステップS60において、ポータブルデバイス6のCPU53は、USBコネクタ56を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ61に記憶させる。

【0217】ステップS61において、移動管理プロ

ラム134は、さらに、利用条件変換プログラム139に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス6が管理している形式に変換する。ステップS62において、移動管理プログラム134は、さらに、利用条件変換プログラム139に、選択されたコンテンツの曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス6の管理する形式に変換させる。そして、ステップS63において、移動管理プログラム134は、PD用ドライバ143に、ステップS61で変換した再生条件と、ステップS62で変換したSCMS情報を、ポータブルデバイス6に転送させる。ポータブルデバイス6のCPU53は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ61に保存する。

【0218】ステップS64において、移動管理プログラム134はまた、PD用ドライバ143に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU11が曲データベース中で扱っている形式のまま、ポータブルデバイス6に転送させ、フラッシュメモリ61に保存させる。

【0219】ステップS65において、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップS66において、復号プログラム142に、その暗号鍵をRAM13に保存されている保存用鍵で復号させ、暗号化プログラム137に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム134は、PD用ドライバ143に、ポータブルデバイス6へ転送させる。

【0220】ポータブルデバイス6のCPU53は、ステップS67で、パーソナルコンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ61に保存する。

【0221】CPU53は、暗号鍵の保存が完了すると、ステップS68において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1の移動管理プログラム134は、ポータブルデバイス6からこの通知を受けると、ステップS69において、コンテンツデータベース114に、そのコンテンツに対応するコンテンツファイル161を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル162）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS70において、移動管理プログラム134は、アダプタ26のCPU32に、曲データベースのデータを転送し、全体

のハッシュ値を計算させ、不揮発性メモリ34に保存させる。このハッシュ値が、上述したステップS52において、前回保存しておいたハッシュ値として用いられることになる。

【0222】次に、パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理は、図12乃至図14のパーソナルコンピュータ1からポータブルデバイス6へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ1においてチェックイン／チェックアウト管理プログラム132により実行され、図14のステップS69において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（またはチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0223】次に、コンテンツ管理プログラム111を実行するCPU11による、図12のステップS55における選択されたコンテンツの再生条件などのチェック処理について図15のフローチャートを参照して説明する。ステップS81において、移動管理プログラム134は、コンテンツデータベース114に、曲データベースから、各種の条件を読み出させる。移動管理プログラム134は、ステップS82において、ステップS81で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎているか否かを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS83に進み、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ20に表示させ、処理を終了させる。ステップS82において、コピー回数がコピー制限回数を過ぎていると判定された場合、ステップS84に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ26のRTC35より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ1の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム134は、この現在日時をCPU32から提供を受けて、ステップS84の判断を自ら行うか、または、ステップS81で、曲データベースから読み出した再生条件をアダプタ26のCPU32に供給し、CPU32に、ステップS84の判定処理を実行させる。

【0224】現在日時が再生終了日時を過ぎている場合、ステップS85に進み、移動管理プログラム134

は、コンテンツデータベース114に、選択されたコンテンツをHDD21から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップS86において、移動管理プログラム134は、CPU32に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ34に保存させる。以後、処理は終了される。従って、この場合、コンテンツの移動が実行されない。

【0225】ステップS84において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップS87に進み、移動管理プログラム134は、その選択されたコンテンツの再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム134は、ステップS88において、PD用ドライバ143に、ポータブルデバイス6と通信させ、ポータブルデバイス6に課金機能が存在するか否かを判定する。ポータブルデバイス6に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス6に転送する訳にはいかないので、ステップS89において、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ20に表示させ、コンテンツの移動処理を終了させる。

【0226】ステップS87において再生時課金条件が登録されていないと判定された場合、または、ステップS88において、ポータブルデバイス6に課金機能が存在すると判定された場合、ステップS90に進み、移動管理プログラム134は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS91に進み、移動管理プログラム134は、ポータブルデバイス6に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス6が、その再生条件を守る機能を有していない場合には、ステップS92に進み、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ20に表示させ、処理を終了させる。

【0227】ステップS90において、再生条件が登録されていないと判定された場合、またはステップS91において、ポータブルデバイス6が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図12のステップS56に戻る。

【0228】図16は、ポータブルデバイス6が管理している（守ることが可能な）再生条件の例を表している。図16に示す再生情報は、例えば、EEPROM68に記憶されている。この例においては、アイテム1乃至アイ

10

20

30

40

50

テム3の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム2についてのみ登録されており、アイテム1とアイテム3については登録されていない。従って、アイテム2のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム1またはアイテム3のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

【0229】次に、図17のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、図12のステップS58におけるフォーマット変換処理の詳細について説明する。ステップS101において、移動管理プログラム134は、コンテンツデータベース114に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップS102において、移動管理プログラム134は、相手先の機器（今の場合、ポータブルデバイス6）に設定することが可能な条件を調べる。すなわち、移動管理プログラム134は、ポータブルデバイス6のCPU53に設定可能な条件を問い合わせ、その回答を得る。ステップS103において移動管理プログラム134は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップS102で調べた条件に基づいて決定する。

【0230】ステップS104において、移動管理プログラム134は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、コンテンツをポータブルデバイス6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス6が守ることができないので、そのようなポータブルデバイス6には、コンテンツを移動することが禁止されるのである。

【0231】ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進み、移動管理プログラム134は、利用条件変換プログラム139に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス6に転送する際、ヘッダに格納される条件）に変換させる。そして、ステップS107において、移動管理プログラム134は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス6は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

【0232】次に、図18乃至図20のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6にコンテンツ

をコピーする場合の処理について説明する。この図18乃至図20のステップS111乃至ステップS127の処理は、コピー管理プログラム133により実行され、図12乃至図14のHDD21からポータブルデバイス6へコンテンツを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス6と、パーソナルコンピュータ1との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ1のHDD21からポータブルデバイス6のフラッシュメモリ61に転送され、保存される。その後、ステップS128において、コピー管理プログラム133は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、コピー管理プログラム133は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0233】次に、図21のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21にコンテンツを移動する処理およびチェックインの処理について説明する。

【0234】始めに、コンテンツの移動の処理について説明する。ステップS161において、移動管理プログラム134は、ポータブルデバイス6のCPU53に対してフラッシュメモリ61に記憶されているコンテンツの情報の読み出しを要求する。CPU53は、この要求に対応して、フラッシュメモリ61に記憶されているコンテンツの情報をパーソナルコンピュータ1に送信する。移動管理プログラム134は、この情報に基づいて、ディスプレイ20に、フラッシュメモリ61に記憶されているコンテンツを選択するためのGUIを表示させる。使用者は、キーボード18またはマウス19を操作して、そのGUIに基づいて、ポータブルデバイス6からHDD21（コンテンツデータベース114）に移動させるコンテンツを指定する。

【0235】ステップS162において、移動管理プログラム134は、認証プログラム141に、CPU53との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図12のステップS56における場合と同様の処理である。

【0236】次に、ステップS163において、CPU53は、フラッシュメモリ61に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ1に転送する。移動管理プログラム134は、ステップS164において、ポータブルデバイス6から転送されてきたコンテンツを、1つのファイルとしてファイル名を付けて、コンテンツデータベース114（HDD21）に保存する。この保存は、例えば、1つの

ファイルの一部として、ファイル名の位置情報（例えば、先頭からのバイト数）を与えて行うようにすることもできる。

【0237】ステップS165において、CPU53は、フラッシュメモリ61に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図14のステップS67の処理でフラッシュメモリ61に保存されていたものである。

【0238】ステップS166において、移動管理プログラム134は、ポータブルデバイス6から暗号鍵の転送を受けると、復号プログラム142に、それを通信用鍵で復号させ、暗号化プログラム137に、自分自身の保存用鍵で暗号化させる。ステップS167で、移動管理プログラム134は、コンテンツデータベース114に、ステップS164で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がGUIを介して入力した曲名、ステップS166で暗号化した暗号鍵などを、HDD21の曲データベースに登録させる。そして、ステップS168において、移動管理プログラム134は、利用条件管理プログラム140に、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0239】ステップS169において、移動管理プログラム134は、ポータブルデバイス6に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU53は、パーソナルコンピュータ1から、そのコンテンツの削除が要求されてきたとき、ステップS170において、フラッシュメモリ61に記憶されているそのコンテンツを削除する。

【0240】次に、ポータブルデバイス6からパーソナルコンピュータ1にコンテンツをチェックインする処理について説明する。ポータブルデバイス6からパーソナルコンピュータ1にコンテンツをチェックインする処理は、図21のポータブルデバイス6からパーソナルコンピュータ1へコンテンツを移動させる場合と同様の処理である。すなわち、チェックインの処理は、パーソナルコンピュータ1においてチェックイン/チェックアウト管理プログラム132により実行され、図21のステップS162乃至S166の処理が省略される。また、パーソナルコンピュータ1は、図21のステップS167において、曲データベースに登録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、ステップS170の処理の後、コンテンツファイルの削除を確認することを出て、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0241】なお、ポータブルデバイス6のフラッシュメモリ61がメモリカードとして着脱可能であるとき、

パーソナルコンピュータ1は、チェックインの処理において、図21のステップS162の相互認証の処理を実行する。

【0242】また、前述のように、所定のパーソナルコンピュータからチェックアウトされたコンテンツが、該パーソナルコンピュータにのみチェックインできるようになっており、チェックイン処理の前処理として、選択されたコンテンツが、チェックインを行うPCからチェックアウトされたかを判断し、該PCからチェックアウトされたものではないと判断されたらば、チェックインを行わないように処理するステップが存在する。例えば、図5のフィールド213の×がついたコンテンツをチェックインしようとした場合がそれにあたる。

【0243】次に、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21へコンテンツをコピーする場合の処理について、図22のフローチャートを参照して説明する。この図22に示すステップS181乃至ステップS188の処理は、図21のポータブルデバイス6からHDD21へコンテンツを移動させる場合の処理におけるステップS161乃至ステップS168の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム133により実行され、図21のステップS169、S170の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【0244】次に、図23のフローチャートを参照して、EMDサーバ4およびコンテンツ管理プログラム111を実行するCPU11による、EMDサーバ4から転送を受けたコンテンツをHDD21にコピーする処理について説明する。ステップS201において、購入用プログラム144は、図5に示すボタン202がクリックされて、使用者からEMDサーバ4へのアクセスが指令されたとき、通信部25を制御し、ネットワーク2を介してEMDサーバ4にアクセスさせる。EMDサーバ4は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク2を介してパーソナルコンピュータ1に転送する。購入用プログラム144は、通信部25を介して、この情報を取得したとき、表示操作指示プログラム112に、それをインタフェース17を介してディスプレイ20に表示させる。使用者は、ディスプレイ20に表示されたGUIを利用して、ステップS202において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク2を介してEMDサーバ4に転送される。ステップS203において、購入用プログラム144は、EMDサーバ4との間において、ネットワーク2を介して相互認証処理を実行し、通信用鍵を共有する。

【0245】パーソナルコンピュータ1とEMDサーバ4との間で行われる相互認証処理は、例えば、ISO 97

98-3で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ1は、自分自身の秘密鍵とEMDサーバ4の公開鍵を予め有しており、EMDサーバ4は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ1の公開鍵は、EMDサーバ4から転送したり、あるいはパーソナルコンピュータ1に予め配布されている証明書(certificate)をパーソナルコンピュータ1からEMDサーバ4に転送し、その証明書をEMDサーバ4が確認し、公開鍵を得るようにしてもよい。さらに、ステップS204において、購入用プログラム144は、EMDサーバ4との間において課金に関する処理を実行する。この課金の処理の詳細は、図24のフローチャートを参照して後述する。

【0246】次に、ステップS205において、EMDサーバ4は、パーソナルコンピュータ1に対して、ステップS202で指定された、暗号化されているコンテンツをネットワーク2を介してパーソナルコンピュータ1に転送する。このとき、時刻情報も適宜転送される。ステップS206において、購入用プログラム144は、コンテンツデータベース114に、転送を受けたコンテンツにファイル名を付けてHDD21に1つのコンテンツファイル161として保存させる。ステップS207において、EMDサーバ4は、さらに、そのコンテンツの暗号鍵をステップS203でパーソナルコンピュータ1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ1へ転送する。

【0247】購入用プログラム144は、ステップS208において、復号プログラム142に、EMDサーバ4より転送を受けた暗号鍵を単独で、またはアダプタ26のCPU32と共同して通信用鍵を用いて復号させ、暗号化プログラム137に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップS209において、購入用プログラム144は、コンテンツデータベース114に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD21の曲データベースに登録させる。さらに、ステップS210において、購入用プログラム144は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0248】なお、ステップS205においてEMDサーバ4は、コンテンツとともに、時刻データをパーソナルコンピュータ1に送信する。この時刻データは、パーソナルコンピュータ1からアダプタ26に転送される。アダプタ26のCPU32は、パーソナルコンピュータ1より転送されてきた時刻データを受信すると、ステップS211において、RTC35の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ26のRTC35の時刻情報を修正するようにしたので、ア

ダプタ26を常に正しい時刻情報を保持することが可能となる。

【0249】次に、図24のフローチャートを参照して、EMDサーバ4およびコンテンツ管理プログラム111を実行するCPU11による、図23のステップS204における課金に関する処理の詳細について説明する。ステップS221において、購入用プログラム144は、ステップS201でEMDサーバ4から伝送されてきた価格情報の中から、ステップS202で指定された選択されたコンテンツの価格情報を読み取り、これをHDD21上の課金ログに書き込む。図25は、このような課金ログの例を表している。この例においては、使用者は、アイテム1乃至アイテム3を、EMDサーバ4からコピーしており、アイテム1とアイテム2の領域は50円とされ、アイテム3の料金は60円とされている。その時点における課金ログのハッシュ値も、CPU32により計算され、不揮発性メモリ34に登録されている。

【0250】次に、ステップS222において、購入用プログラム144は、ステップS221で書き込んだ課金ログをHDD21から読み出し、これをネットワーク2を介してEMDサーバ4に転送する。EMDサーバ4は、ステップS223において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ4は、内蔵するデータベースに、パーソナルコンピュータ1の使用者から伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ4は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ4は、決裁に必要な商品名、金額などを決裁サーバ(図示せず)に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

【0251】次に、図26と図27のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、音声入出力インタフェース24のIEC60958端子24aから入力された、図示せぬCDプレーヤなどからの再生されたコンテンツを、HDD21にコピーする場合の処理について説明する。ステップS241において、使用者は、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インタフェース24のIEC60958端子24aに接続する。ステップS242において、使用者は、キーボード18またはマウス19を操作し、CDプレーヤからコピーするコンテンツの曲名(または、コンテンツに対応する番号)を入力する。そして、ステップS243において使用者は、CDプレーヤ

のボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1のキーボード18またはマウス19を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【0252】CDプレーヤにおいて、CDの再生が開始されると、ステップS244において、CDプレーヤから出力されたコンテンツが、IEC60958端子24aを介してパーソナルコンピュータ1に転送されてくる。ステップS245において、コピー管理プログラム133は、IEC60958端子24aを介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー1回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップS246において、CPU11は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップS247に進み、コピー管理プログラム133は、表示操作指示プログラム112に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ20に表示させ、コピー処理を終了する。すなわち、この場合には、HDD21へのコピーが禁止される。

【0253】コピー管理プログラム133は、ステップS246において、ステップS245で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップS248に進み、ウォータマークコードを読み出し、そのウォータマークがコピー禁止を表しているか否かをステップS249において判定する。ウォータマークコードがコピー禁止を表している場合には、ステップS247に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【0254】ステップS249において、ウォータマークがコピー禁止を表していないと判定された場合、ステップS250に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップS251、S252の処理で、処理が終了される。この処理は、図7のステップS13、S14の処理と同様の処理である。

【0255】選択されたコンテンツがまだHDD21に登録されていないコンテンツであれば、ステップS253乃至S258で、その登録処理が実行される。このステップS253乃至ステップS258の処理は、ステップS257において、IEC60958端子24aから供給されてくるSCMS情報も曲データベースに登録される点を除き、図7のステップS19乃至ステップS24の処理と同様の処理であるので、その説明は省略する。

【0256】次に、図28と図29のフローチャートを参照して、コンテンツ管理プログラム111を実行する

CPU11による、コンテンツをHDD21からIEC60958端子24aに出力(再生)する場合の処理について説明する。ステップS271乃至ステップS273において、図18のステップS111乃至S113における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS274に進み、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、HDD21の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、ディスプレイ20に表示させる。使用者は、その表示を見て、キーボード18またはマウス19を適宜操作して、再生出力するコンテンツを選択する。ステップS275において、表示操作指示プログラム112は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図30のフローチャートを参照して後述する。

【0257】次に、ステップS276において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、ステップS274において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム142に保存用鍵で復号させる。ステップS277において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツのSCMS情報を曲データベースから読み出させ、IEC60958端子24aから出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけインクリメントされ、新たなSCMS情報とされる。ステップS278において、表示操作指示プログラム112はさらに、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツのISRCを曲データベースから読み出させる。

【0258】次に、ステップS279において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツをHDD21から読み出させる。表示操作指示プログラム112はさらに、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム142に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮/伸張プログラム138は、さらに、そのコンテンツの圧縮符号を復号(伸張)する。ステップS280において、表示操作指示プログラム112は、ドライ

パ117に、ステップS279で、復号したデジタルデータであるコンテンツを、ステップS277で決定したSCMS情報、並びにステップS278で読み出したISRC情報とともに、IEC60958の規定に従って、IEC60958端子24aから出力させる。さらにまた、表示操作指示プログラム112は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インタフェース24のアナログ出力端子から出力させる。

【0259】ステップS281において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベース中の再生回数カウンタの値を1だけインクリメントさせる。そして、ステップS282において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS283に進み、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、対応する料金を課金ログに書き込ませ、ステップS284において、表示操作指示プログラム112は、利用条件管理プログラム140に、曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に記憶させる。ステップS282において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップS283とステップS284の処理はスキップされる。

【0260】次に、図30のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、図28のステップS275の再生条件等のチェック処理の詳細について説明する。ステップS301において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベースの各種条件を読み出させる。ステップS302において利用条件管理プログラム140は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS303に進み、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツをHDD21から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップS304において、表示操作指示プログラム112はさらに、利用条件管理プログラム140に、曲データベースの新たなハッシュ値をCPU32に計算させ、そのハッシュ値を不揮発性メモリ34に保存させる。この場合、再生出力は禁止される。

【0261】ステップS302において、再生回数が制限回数を過ぎていると判定された場合、ステップS305に進み、利用条件管理プログラム1402は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した

場合と同様にステップS303において、選択されたコンテンツをHDD21から削除させるとともに、曲データベースからも削除させる。そして、ステップS304において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【0262】ステップS305において、再生終了日時が現在日時を過ぎていないと判定された場合は、ステップS306に進み、CPU32は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS307に進み、表示操作指示プログラム112は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ20に表示させる。ステップS306において、再生時課金条件が付加されていないと判定された場合、ステップS307の処理はスキップされる。

【0263】次に、図31と図32のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6経由でコンテンツを出力（再生）する場合の処理について説明する。ステップS321乃至ステップS325において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図28のステップS271乃至ステップS275の処理と同様の処理であるので、その説明は省略する。

【0264】ステップS326において、ポータブルデバイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS327において、表示操作指示プログラム112は、ポータブルデバイス6に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップS328において、表示操作指示プログラム112は、ステップS324で、コンテンツ管理プログラム111を介してコンテンツデータベース114に、指定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD21から読み出させる。表示操作指示プログラム112は、ステップS329において、コンテンツ管理プログラム111に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス6の方式のものに変換する処理を実行させる。そして、ステップS330において、表示操作指示プログラム112は、暗号化プログラム137に、ステップS329において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス6に転送する。

【0265】ステップS331において、ポータブルデバイス6のCPU53は、ステップS327において、バ

パーソナルコンピュータ 1 から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップ S 3 3 2 において、表示操作指示プログラム 1 1 2 は、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 に、曲データベースの再生回数カウンタを 1 だけインクリメントさせる。さらに、ステップ S 3 3 3 において、表示操作指示プログラム 1 1 2 は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップ S 3 3 4 において、コンテンツ管理プログラム 1 1 1 を介してコンテンツデータベース 1 1 4 に、その料金を課金ログに書き込ませ、ステップ S 3 3 5 において、CPU 3 2 に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップ S 3 3 4、ステップ S 3 3 5 の処理はスキップされる。

【0266】本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU 1 1 を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパレジスタントソフトウェアとされている。

【0267】さらに、上述したように、CPU 1 1 の機能の一部は、ハードウェアとしてのアダプタ 2 6 に分担され、両者が共働して各種の処理を実行するようになっている。これにより、より安全性を高めることが可能となっている。

【0268】例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ 2 6 の不揮発性メモリ 3 4 に保存される。すなわち、図 8 のステップ S 3 2、S 3 3 などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ 3 4 に記憶されているものとされる。これにより、例えば、他の記録媒体にコピーまたは移動させる前に、HDD 2 1 に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD 2 1 から、そこに保存されているコンテンツを他の記録媒体にコピーまたは移動した後、HDD 2 1 にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピーまたは移動ができてしまうようなことが防止される。

【0269】例えば、図 3 3 に示すように、HDD 2 1 にコンテンツ A、B が保存されている場合、不揮発性メモリ 3 4 には、コンテンツ A とコンテンツ B の情報に対応するハッシュ値が保存されている。この状態において、HDD 2 1 のコンテンツ A、B を含む記録データの一部または全部を他の記録媒体 2 7 1 にバックアップしたとする。その後、HDD 2 1 に保存されているコンテンツ A とコンテンツ B のうち、コンテンツ A を他の記録媒体 2 7

2 に移動させた場合、その時点において、HDD 2 1 に記録されているコンテンツは、コンテンツ B だけとなるので、不揮発性メモリ 3 4 のハッシュ値も、コンテンツ B に対応するハッシュ値に変更される。

【0270】従って、その後、記録媒体 2 7 1 にバックアップしておいた HDD 2 1 のコンテンツ A、B を含む記録データの一部または全部を HDD 2 1 にリストアして、HDD 2 1 に、再びコンテンツ A とコンテンツ B を保存させたとしても、不揮発性メモリ 3 4 には、コンテンツ B の情報から演算されたハッシュ値が記憶されており、コンテンツ A とコンテンツ B の情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 2 1 に記憶されているコンテンツ A とコンテンツ B に基づくハッシュ値が、不揮発性メモリ 3 4 に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 2 1 に保存されているコンテンツ A とコンテンツ B の利用が制限されてしまうことになる。

【0271】さらに、上述したように、アダプタ 2 6 は、RTC 3 5 を内蔵しており、この RTC 3 5 の値は、正しい認証結果が得られた他の装置（例えば、EMD サーバ 4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ 1 が管理するものではなく、RTC 3 5 が出力するものが利用される。従って、使用者が、パーソナルコンピュータ 1 の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【0272】また、アダプタ 2 6 は、暗号化されて転送されてきたプログラムを ROM 3 6 に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図 3 4 のフローチャートを参照して説明する。

【0273】すなわち、パーソナルコンピュータ 1 は、アダプタ 2 6 に対して、所定の処理を実行させたいとき、ステップ S 3 5 1 において、アダプタ 2 6 に実行させるべきプログラムを RAM 1 3 に予め記憶されている暗号鍵を用いて暗号化してアダプタ 2 6 に転送する。アダプタ 2 6 の ROM 3 6 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU 3 2 は、この ROM 3 6 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 3 5 2 において復号する。そして、ステップ S 3 1 3 において、CPU 3 2 は、復号したプログラムを RAM 3 3 に展開し、ステップ S 3 5 4 において、そのプログラムを実行する。

【0274】例えば、上述したように、パーソナルコンピュータ 1 の CPU 1 1 は、HDD 2 1 の曲データベースのハッシュ値をアダプタ 2 6 に計算させるとき、曲データベ

ースのデータを暗号鍵で暗号化してアダプタ26のCPU32に転送する。CPU32は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ34に記憶させる。あるいは、そのハッシュ値を、CPU32は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ1のCPU11に転送する。

【0275】図35は、アダプタ26の内部のより具体的な構成を表している。アダプタ26は、半導体ICとして形成される。アダプタ26は、図2に示したインタフェース31、CPU32、RAM33、不揮発性メモリ34、RTC35、ROM36以外に、RAM33に対する書き込みと読み出しを制御するRAMコントローラ301、並びに論理回路302を有している。論理回路302は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ26から直接出力するような場合の処理のために用いられる。

【0276】これらのインタフェース31乃至ROM36、RAMコントローラ301、並びに論理回路302は、半導体IC内に一体的に組み込まれ、外部からは分解できないように構成されている。

【0277】水晶振動子311は、アダプタ26が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路312は、RTC35を動作させるための発振回路である。バッテリー313は、発振回路312、不揮発性メモリ34、およびRTC35に対してバックアップ用の電力を供給している。アダプタ26のその他の回路には、パーソナルコンピュータ1の電源供給回路321からの電力が供給されている。

【0278】不揮発性メモリ34は、書き込み消去可能なROMで構成することも可能であるが、バッテリー313からのバックアップ電源でバックアップされるRAMで構成する場合には、例えば、図36に示すように、不揮発性メモリ34の上に保護アルミニウム層351を形成し、さらに、その保護アルミニウム層351と同一平面上となるように、不揮発性メモリ34にバッテリー313からの電力を供給する電源パターン352を形成することができる。このようにすると、例えば、不揮発性メモリ34を改竄すべく、保護アルミニウム層351を削除しようとする、同一平面上の電源パターン352も削除されてしまい、不揮発性メモリ34に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【0279】さらに、図37に示すように、不揮発性メモリ34に対するデータの書き込みまたは読み出しのための配線401-1乃至401-3は、対応する位置で、上下(深さ)方向に重なりあうように形成されている。これにより、より下層の配線401-3からデータ

を読み出すためには、上方の配線401-1、401-2を除去しなければならず、複数の配線401-1、401-2、401-3から同時にデータを読み取ることができなくなる。

【0280】さらにまた、不揮発性メモリ34は、配線401-1乃至401-3を冗長に形成するようにすることができる。例えば、不揮発性メモリ34内部に形成される配線401-1乃至401-3が不揮発性メモリ34を構成するトランジスタなどの素子を結合するとき、その経路は、例えば、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにすることで、配線401-1乃至401-3の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

【0281】不揮発性メモリ34からデータを読み出すために設計されている専用の回路(半導体ICとしてのアダプタ26に内蔵されている)は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ34が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ34に記憶されているデータを読み出すべく、プローブを配線401-1乃至401-3に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

【0282】以上においては、記録媒体として、ポータブルデバイス6を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【0283】また、コンテンツは、曲のデータまたは音声データなどの楽音データ以外に、画像データ、その他のデータとすることもできる。

【0284】以上のように、本発明によれば、次のような効果を奏することができる。

【0285】(1) HDD21に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上でHDD21に記録するようにしたので、HDD21に記録されているコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【0286】(2) 所定の曲を1回コピーしたとき、一定時間(上記例の場合、48時間)の間、その曲をコピーすることができないようにするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【0287】さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0288】(3) 外部の装置にコンテンツを渡した

ら、HDD2 1上のコンテンツを消去するようにしたので、HDD2 1内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

【0289】(4) HDD2 1内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD2 1の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD2 1にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【0290】(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0291】(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

【0292】(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【0293】(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ26に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【0294】なお、アダプタ26が実行する処理は、セキュアなプログラムでCPU1 1が実行するようにしてもよい。この場合において、例えば、同一な値を有する保存用鍵は、保存用鍵が必要になった時点で、コンテンツ管理プログラム111により生成される。同様に、ハッシュ値は、コンテンツ管理プログラム111により隠蔽されて保存される。

【0295】また、アダプタ26が実行する処理が、セキュアなプログラムでCPU1 1により実行されるとき、パーソナルコンピュータ1は、アダプタ26のRTC35が供給する現在時刻に代えて、ネットワーク2に接続されている特定のサーバ(例えば、EMD登録サーバ3)から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ1は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けられないようにしてもよい。

【0296】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

10 【0297】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図2に示すように、磁気ディスク41(フロッピディスクを含む)、光ディスク42(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク43(MD(Mini-Disc)を含む)、若しくは半導体メモリ44などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM12や、HDD2 1などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部25などのインタフェースを介して、ローカルエリアネットワークまたはインターネットなどのネットワーク2、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0298】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

30 【0299】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0300】

【発明の効果】以上の如く、請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載のプログラム格納媒体によれば、蓄積されているデータを他の装置に移転するとき、他の装置が、データの利用時の条件を充足できるか否かを判定し、その判定結果に基づいて、データの利用時の条件とともにデータを移転するようにしたので、不正な他の装置にデータを移転した後、その装置から、さらに他の装置にデータをコピーするなどして、データが不正に複製されることを確実に防止することが可能となる。

【図面の簡単な説明】

【図1】本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。

【図2】パーソナルコンピュータ1の構成を説明する図である。

【図3】ポータブルデバイス6の構成を説明する図である。

【図4】パーソナルコンピュータ1の機能の構成を説明するブロック図である。

【図5】表示操作指示ウィンドウの例を示す図である。

【図6】録音プログラム113がディスプレイ20に表示させるウィンドウの例を説明する図である。

【図7】コンパクトディスクからHDD21にコンテンツをコピーする場合の処理を説明するフローチャートである。

【図8】図7のステップS12の期限データベースチェック処理を説明するフローチャートである。

【図9】期限データベースの例を示す図である。

【図10】ウォーターマークを説明する図である。

【図11】曲データベースの例を示す図である。

【図12】HDD21からポータブルデバイス6へコンテンツを移動する動作を説明するフローチャートである。

【図13】HDD21からポータブルデバイス6へコンテンツを移動する動作を説明するフローチャートである。

【図14】HDD21からポータブルデバイス6へコンテンツを移動する動作を説明するフローチャートである。

【図15】図12のステップS55の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

【図16】ポータブルデバイス6が管理している再生条件を説明する図である。

【図17】図12のステップS58のフォーマット変換処理の詳細を説明するフローチャートである。

【図18】HDD21からポータブルデバイス6へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図19】HDD21からポータブルデバイス6へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図20】HDD21からポータブルデバイス6へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図21】ポータブルデバイス6からHDD21へコンテンツを移動する場合の動作を説明するフローチャートである。

【図22】ポータブルデバイス6からHDD21へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図23】EMDサーバ4からHDD21へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図24】図23のステップS204の課金に関する処理の詳細を説明するフローチャートである。

【図25】課金ログを説明する図である。

【図26】図2のパーソナルコンピュータ1のIEC60958端子24aからHDD21へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図27】図2のパーソナルコンピュータ1のIEC60958

端子24aからHDD21へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図28】HDD21からIEC60958端子24aにコンテンツを出力する場合の動作を説明するフローチャートである。

【図29】HDD21からIEC60958端子24aにコンテンツを出力する場合の動作を説明するフローチャートである。

【図30】図28のステップS275の再生条件などのチェック処理を説明するフローチャートである。

【図31】HDD21からポータブルデバイス6経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図32】HDD21からポータブルデバイス6経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図33】不揮発性メモリ34の機能を説明する図である。

【図34】アダプタ26の動作を説明するフローチャートである。

【図35】アダプタ26の内部の構成を示す図である。

【図36】不揮発性メモリ34の内部の構成例を示す図である。

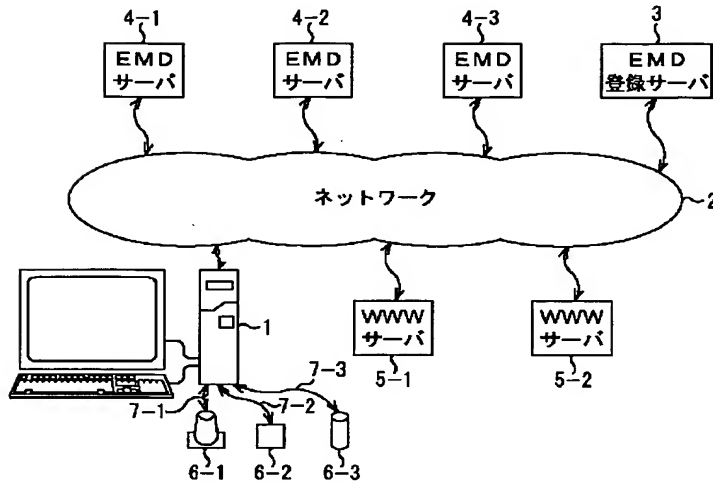
【図37】不揮発性メモリ34の内部の構成例を示す図である。

【符号の説明】

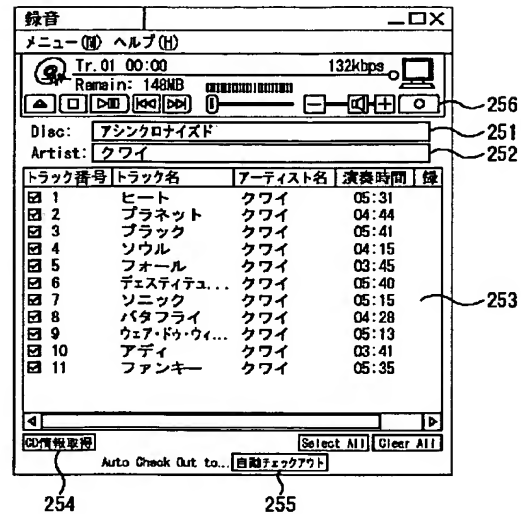
1 パーソナルコンピュータ, 2 ネットワーク, 3 EMD登録サーバ, 6-1乃至6-3 ポータブルデバイス, 11 CPU, 12 ROM, 13 RAM, 21 HDD, 24 音声入出力インターフェース, 24a IEC60958端子, 26 アダプタ, 32 CPU, 33 RAM, 34 不揮発性メモリ, 35 RTC, 36 ROM, 41 磁気ディスク, 42 光ディスク, 43 光磁気ディスク, 44 半導体メモリ, 53 CPU, 54 RAM, 55 ROM, 59 DSP, 61 フラッシュメモリ, 111 コンテンツ管理プログラム, 112 表示操作指示プログラム, 113 録音プログラム, 114 コンテンツデータベース, 131 EMD選択プログラム, 132 チェックイン/チェックアウト管理プログラム, 133 コピー管理プログラム, 134 移動管理プログラム, 135 暗号方式変換プログラム, 136 圧縮方式変換プログラム, 137 暗号化プログラム, 138 圧縮/伸張プログラム, 139 利用条件変換プログラム, 140 利用条件管理プログラム, 141 認証プログラム, 142 復号プログラム, 143 PD用ドライバ, 144 購入用プログラム, 145 購入用プログラム, 181 フィルタリングデータファイル, 182 表示データファイル, 183 画像ファイル, 184 履歴データフ

ファイル, 351 保護アルミニウム層, 352 * * 電源パターン, 401-1乃至401-3配線

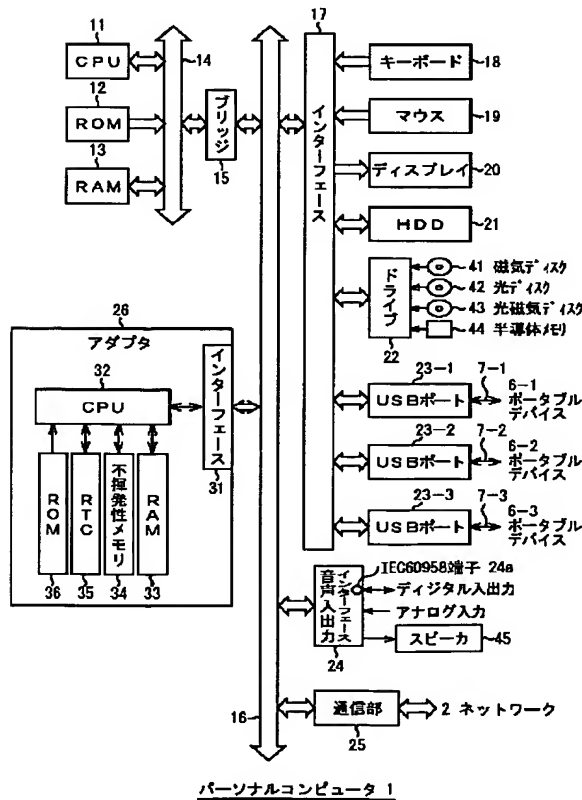
【図1】



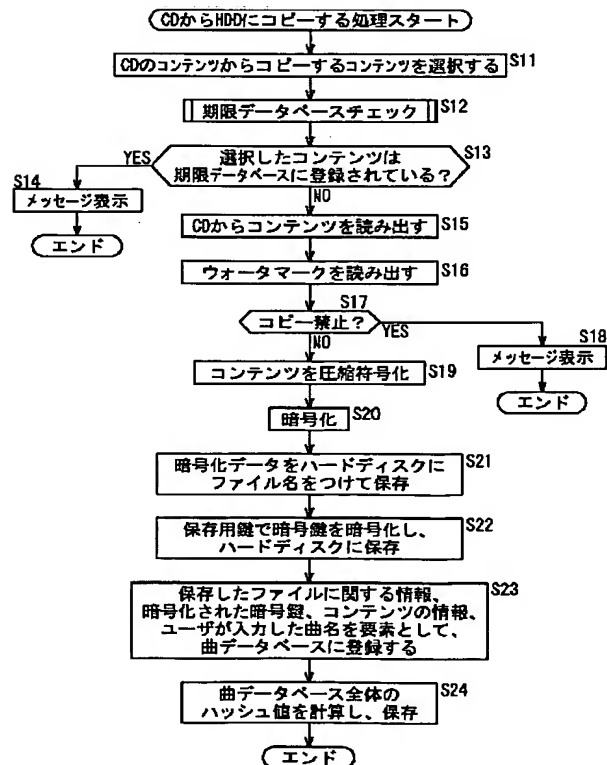
【図6】



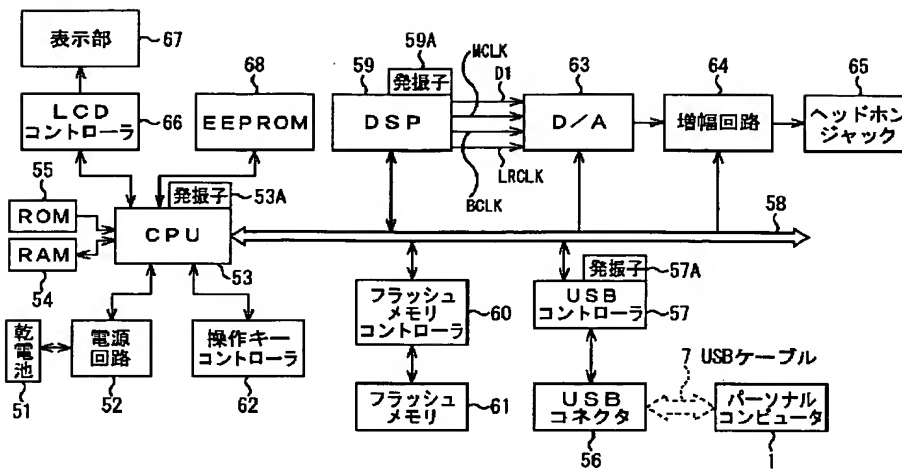
【図2】



【図7】

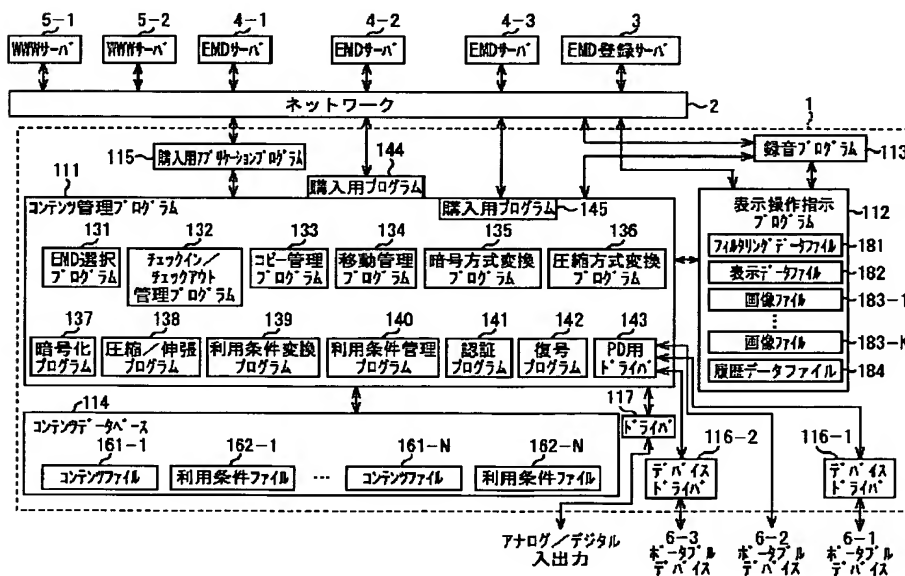


【図 3】



ポータブルデバイス 6

【図4】



【圖 9】

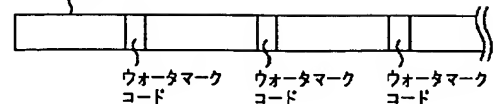
【図 10】

期限データベース

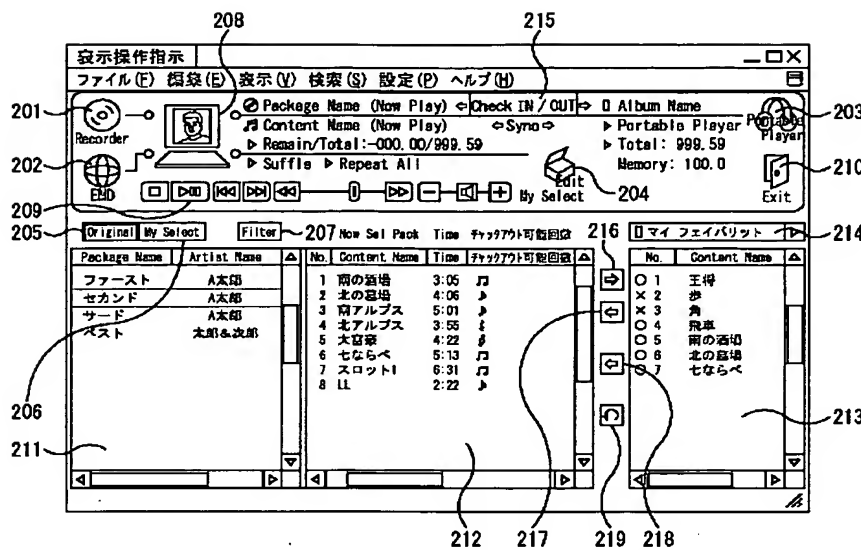
	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934
-------	----------------

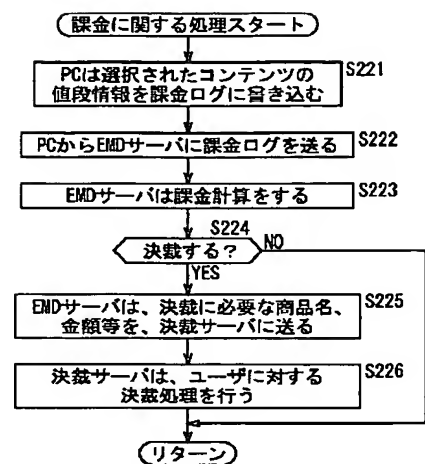
コンテンツ



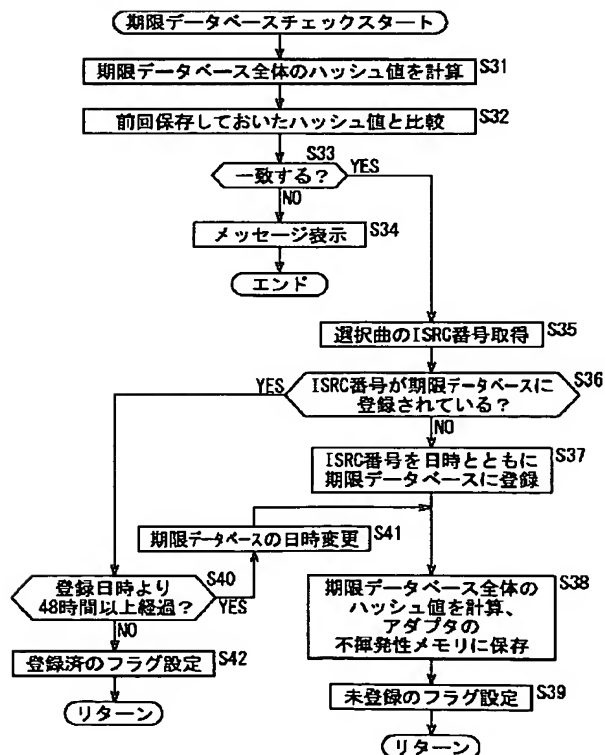
【図5】



【図24】

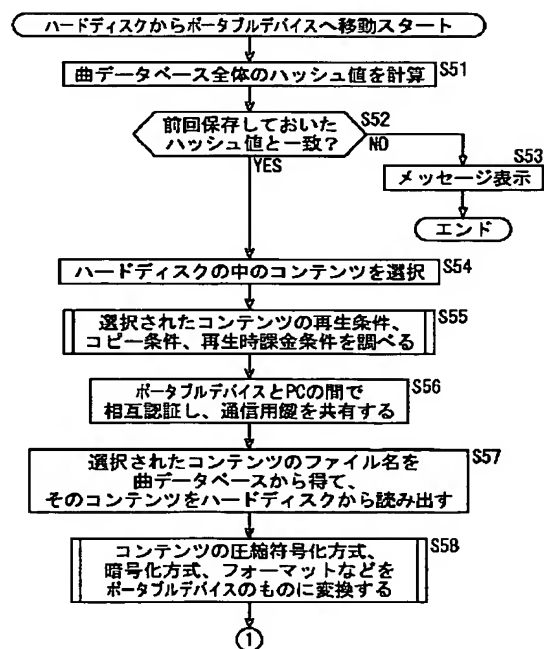


【図8】



【図12】

(12-1)



【図11】

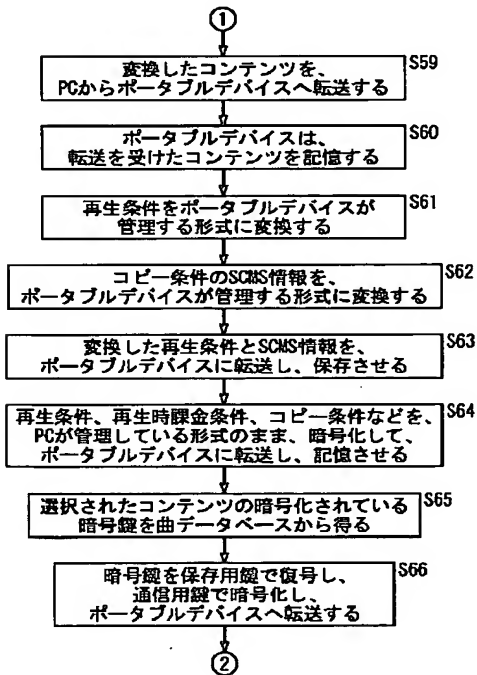
曲データベース

	アイテム1	アイテム2	アイテム3
ファイル名	xd000110. at2	px92341234. at2	aa0234287034. at2
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012
曲名	春の小川	運命	荒城の月
長さ	180	190	200
再生条件:開始日時	-	2001. 01. 01. 00:00	-
再生条件:終了日時	1999. 07. 31. 23:59	-	-
再生条件:回数制限	-	20	-
再生回数カウンタ	-	12	-
再生時課金条件	-	-	¥5
コピー条件:回数	2	0	0
コピー回数カウンタ	1	0	0
コピー条件:SCMS	0b01	0b10	0b00

ハッシュ値 0xf9951e566321

【図13】

(12-2)



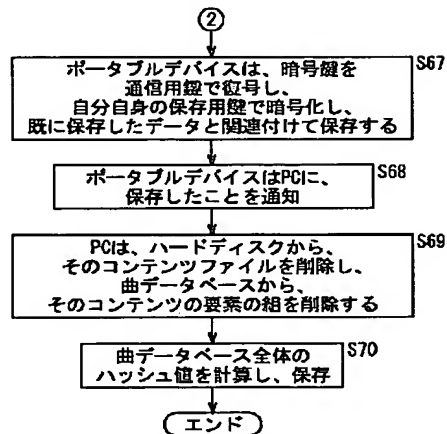
【図16】

ポータブルデバイスが管理している再生条件

	アイテム1	アイテム2	アイテム3
コンテンツID	00001	00002	00003
再生開始日時	1999. 07. 31. 23:59	1999. 07. 31. 23:59	1999. 07. 31. 23:59
再生終了日時	2001. 01. 01. 00:00	2001. 01. 01. 00:00	2001. 01. 01. 00:00
再生回数	-	15	-

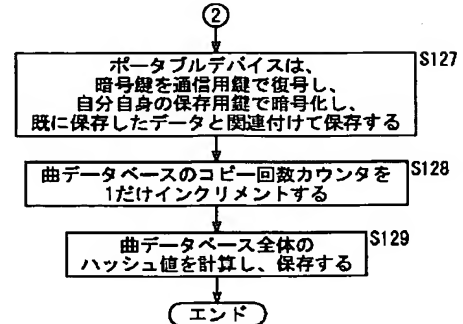
【図14】

(12-3)

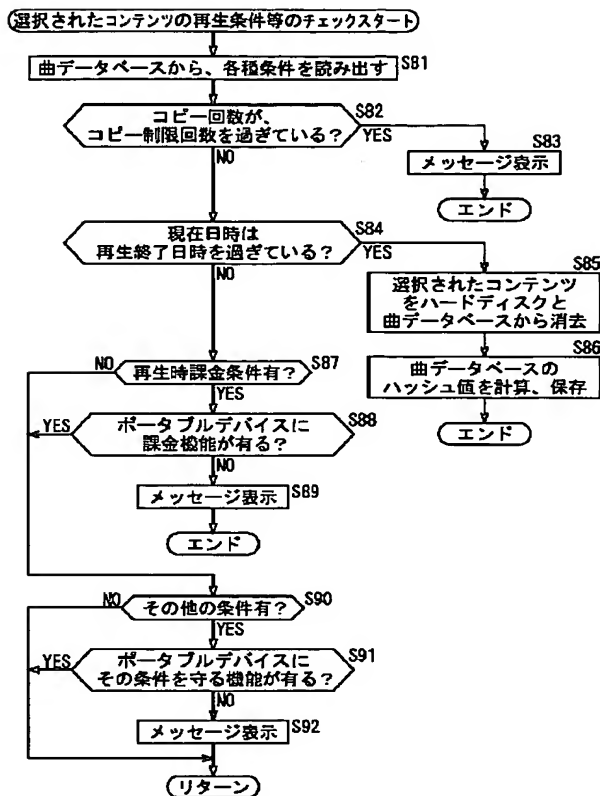


【図20】

(18-3)

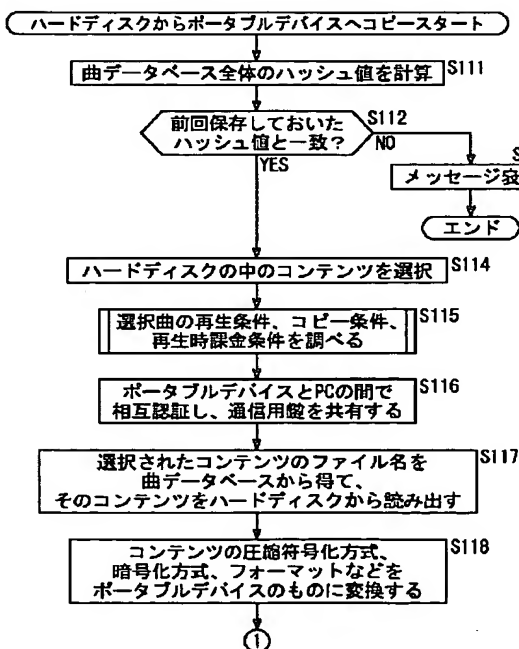


【図15】

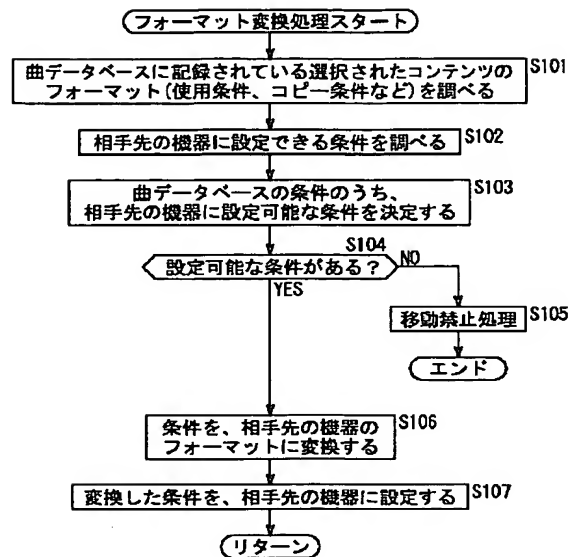


【図18】

(18-1)

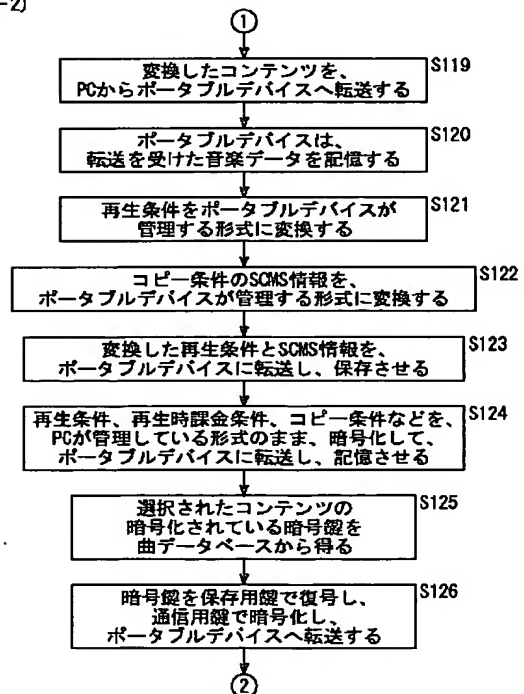


【図17】

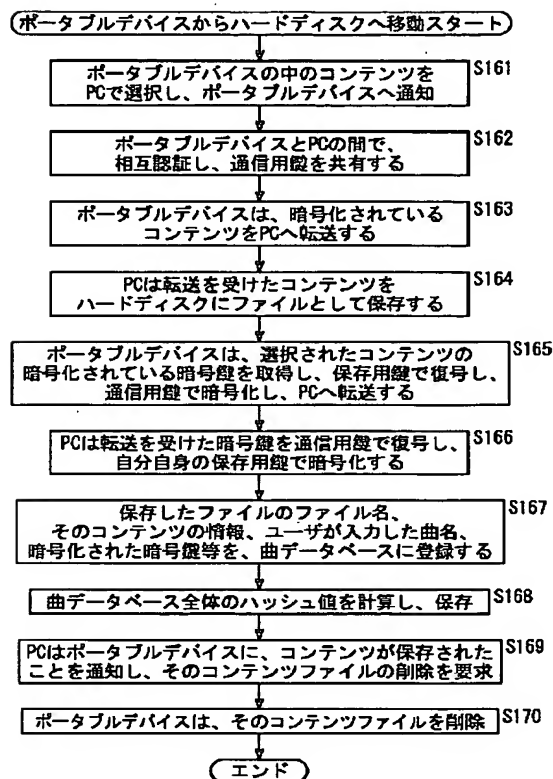


【図19】

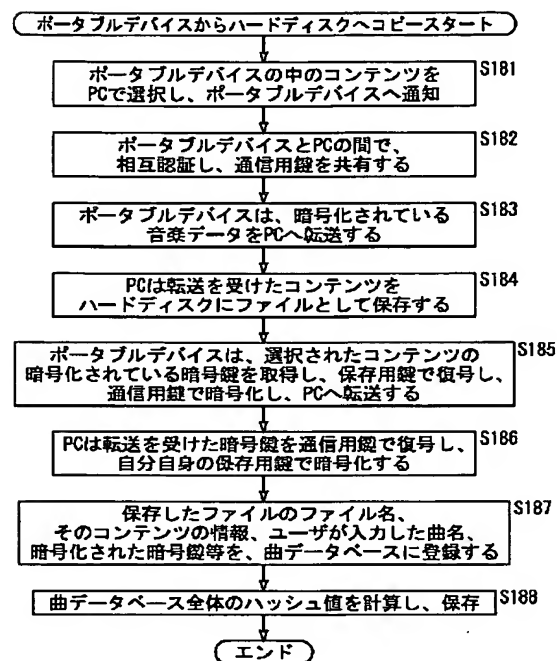
(18-2)



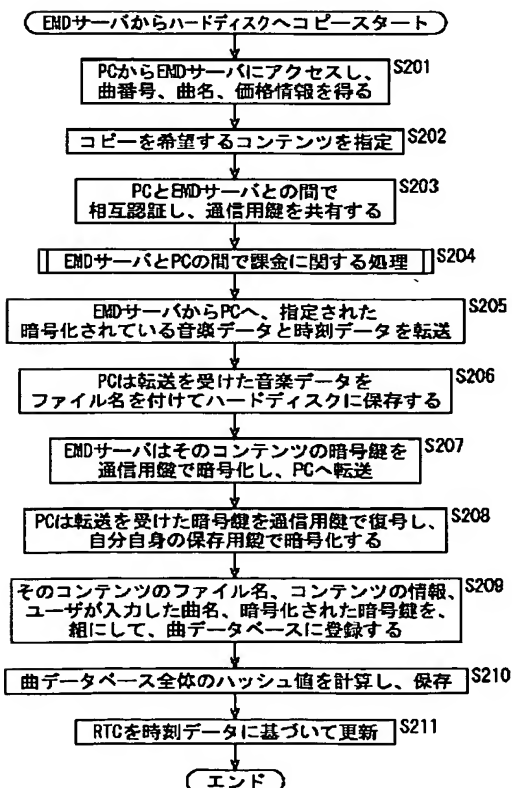
【図21】



【図22】

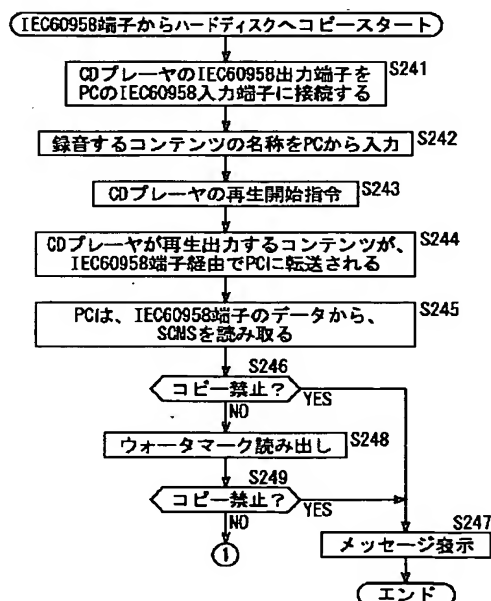


【図23】



【図26】

(26-1)



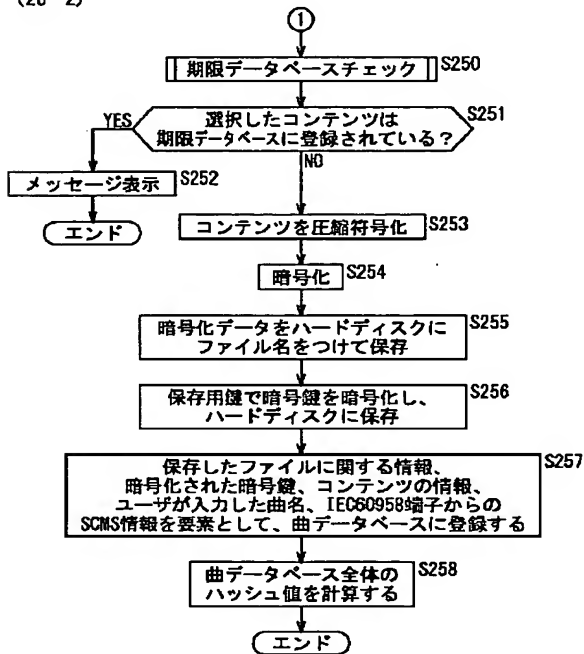
【図25】

課金ログ

	アイテム1	アイテム2	アイテム3	
料金	50	50	60	
ハッシュ値	0xf8783e263517			

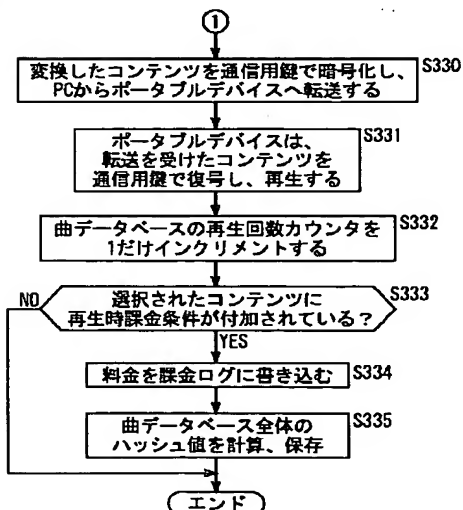
【図27】

(26-2)



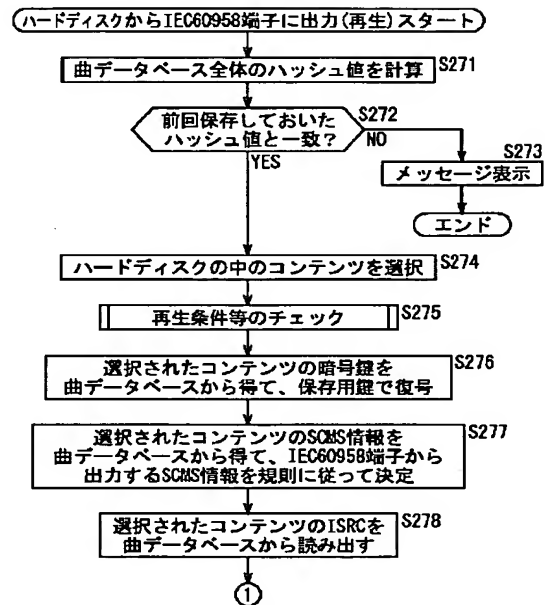
【図32】

(31-2)

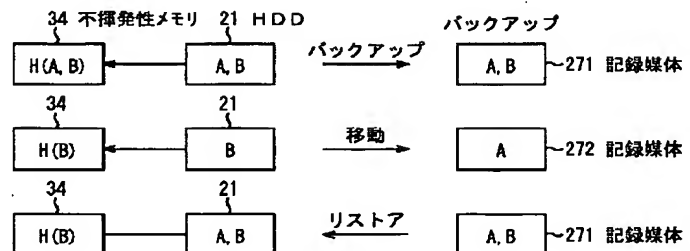


【図28】

(28-1)

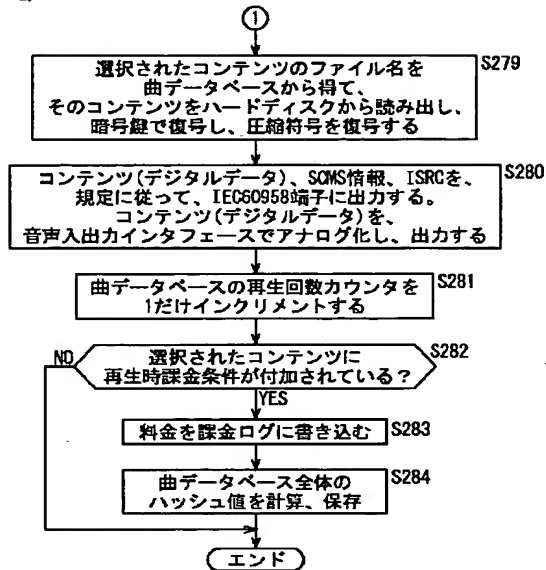


【図33】



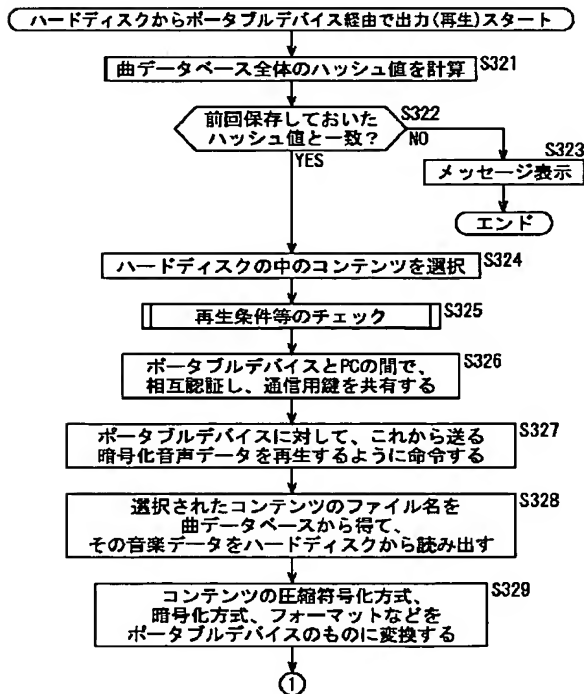
【図29】

(28-2)

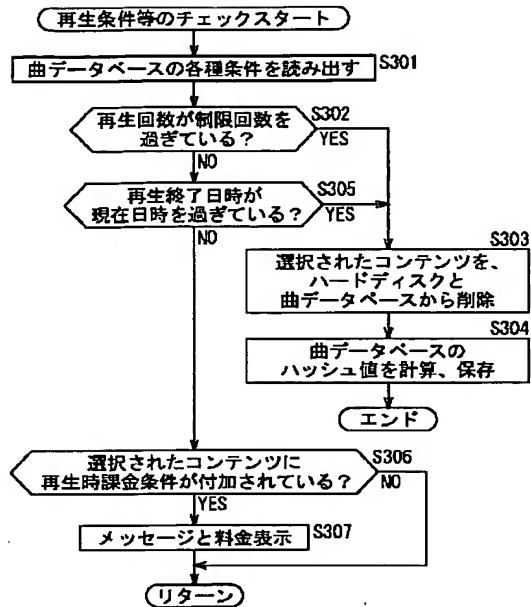


【図31】

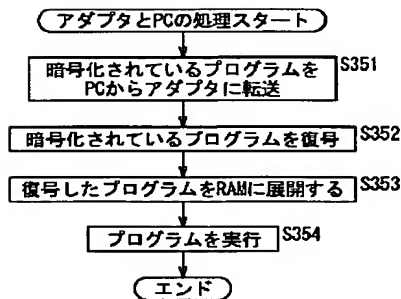
(31-1)



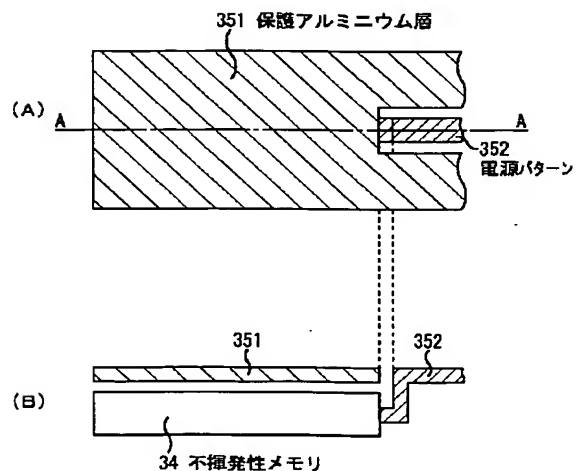
【図30】



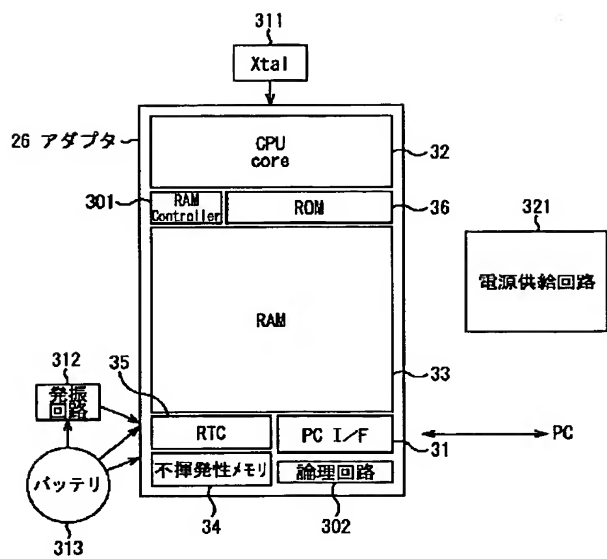
【図34】



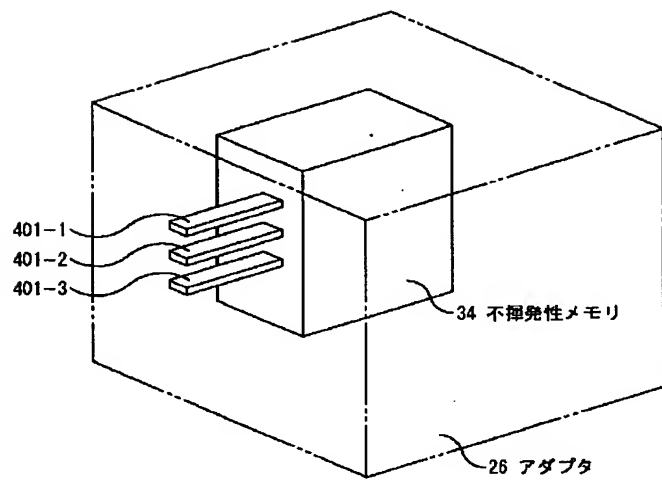
【図36】



【図35】



【図37】



フロントページの続き

(72)発明者 田辺 充
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 江面 裕一
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5B017 AA06 BA07 BB10 CA16
5D044 AB05 AB07 BC01 CC04 CC08
DE50 GK12 HL08